# TigerSwitch 10/100

## Stackable Fast Ethernet Switch

- 24 10BASE-T/100BASE-TX RJ-45 ports
- Auto MDI/MDI-X support on all ports
- Optional 100BASE-FX or 1000BASE-X modules
- Optional stack module for linking up to 16 units
- 8.8 Gbps of aggregate switch bandwidth
- LACP and FEC port trunking support
- Port mirroring for non-intrusive analysis
- Port security
- Full support for IEEE 802.1Q VLANs with GVRP
- IP Multicasting with IGMP Snooping
- Manageable via console, Web, SNMP/RMON

SMC® Networks

## Management Guide

*SMC6624M*

# TigerSwitch 10/100 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC®
Networks
6 Hughes
Irvine, CA 92618
Phone: (949) 707-2400

July 2001
Pub. # 150000001100A R01

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2001 by
SMC Networks, Inc.
6 Hughes
Irvine, CA 92618
All rights reserved. Printed in Taiwan

**Trademarks:**

SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

# LIMITED WARRANTY

**Limited Warranty Statement:** SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/smc/pages_html/support.html.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customers at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

**WARRANTIES EXCLUSIVE:** IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION,

MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
6 Hughes
Irvine, CA 92618

# Contents


## 1 Selecting a Management Interface

**Understanding Management Interfaces** . . . . . 1-1

**Advantages of Using the Menu Interface** . . . . . 1-2

**Advantages of Using the CLI** . . . . . 1-3
CLI Usage . . . . . 1-3

**Advantages of Using the Web Browser Interface** . . . . . 1-4

## 2 Using the Menu Interface

**Starting and Ending a Menu Session** . . . . . 2-2
How To Start a Menu Interface Session . . . . . 2-3
How To End a Menu Session and Exit from the Console: . . . . . 2-4

**Main Menu Features** . . . . . 2-6

**Screen Structure and Navigation** . . . . . 2-8

**Rebooting the Switch** . . . . . 2-11

**Menu Features List** . . . . . 2-13

**Where To Go From Here** . . . . . 2-14

## 3 Using the Command Line Interface (CLI)

**Accessing the CLI** . . . . . 3-1

**Using the CLI** . . . . . 3-1
Privilege Levels at Logon . . . . . 3-2
Privilege Level Operation . . . . . 3-3
Operator Privileges . . . . . 3-3
Manager Privileges . . . . . 3-4
How To Move Between Levels . . . . . 3-6
Listing Commands and Command Options . . . . . 3-7
Listing Commands Available at Any Privilege Level . . . . . 3-7
Command Option Displays . . . . . 3-9
Displaying CLI “Help” . . . . . 3-10
Configuration Commands and the Context Configuration Modes . . 3-12

**CLI Control and Editing** . . . . . 3-15

## 4 Using the Web Browser Interface

**General Features** . . . . . 4-2

**Web Browser Interface Requirements** . . . . . 4-3

**Starting a Web Browser Interface Session with the Switch** . . . . . 4-4

Using a Standalone Web Browser in a PC or UNIX Workstation . . . . 4-4

**Tasks for Your First Web Browser Interface Session** . . . . . 4-6

Viewing the "First Time Install" Window . . . . . 4-6

Creating Usernames and Passwords in the Browser Interface . . . . . 4-7

Using the Passwords . . . . . 4-8

Using the User Names . . . . . 4-9

If You Lose a Password . . . . . 4-9

**Support/Mgmt URL Feature** . . . . . 4-10

Support URL . . . . . 4-10

**Status Reporting Features** . . . . . 4-11

The Overview Window . . . . . 4-11

The Port Utilization and Status Displays . . . . . 4-12

Port Utilization . . . . . 4-12

Port Status . . . . . 4-14

The Alert Log . . . . . 4-15

Sorting the Alert Log Entries . . . . . 4-15

Alert Types . . . . . 4-16

Viewing Detail Views of Alert Log Entries . . . . . 4-17

The Status Bar . . . . . 4-17

## 5 Configuring IP Addressing, Interface Access, and System Information

**IP Configuration** . . . . . 5-2

Just Want a Quick Start? . . . . . 5-3

IP Addressing with Multiple VLANs . . . . . 5-3

IP Addressing in a Stacking Environment . . . . . 5-4

Menu: Configuring IP Address, Gateway, Time-To-Live (TTL), and Timep . . . . . 5-4

CLI: Configuring IP Address, Gateway, Time-To-Live (TTL), and Timep . . . . . 5-6

Web: Configuring IP Addressing . . . . . 5-9
How IP Addressing Affects Switch Operation . . . . . 5-9
DHCP/Bootp Operation . . . . . 5-10
Network Preparations for Configuring DHCP/Bootp . . . . . 5-13
Globally Assigned IP Network Addresses . . . . . 5-14
**Interface Access: Console/Serial Link, Web, and Inbound Telnet** 5-15
Menu: Modifying the Interface Access . . . . . 5-16
CLI: Modifying the Interface Access . . . . . 5-17
**System Information** . . . . . 5-20
Menu: Viewing and Configuring System Information . . . . . 5-21
CLI: Viewing and Configuring System Information . . . . . 5-22
Web: Configuring System Parameters . . . . . 5-24

## 6 Optimizing Port Usage Through Traffic Control and Port Trunking

**Overview** . . . . . 6-1
**Viewing Port Status and Configuring Port Parameters** . . . . . 6-1
Menu: Viewing Port Status and Configuring Port Parameters . . . . . 6-4
CLI: Viewing Port Status and Configuring Port Parameters . . . . . 6-5
Web: Viewing Port Status and Configuring Port Parameters . . . . . 6-8
**Port Trunking** . . . . . 6-9
SMC6624M Port Trunk Features and Operation . . . . . 6-10
Trunk Configuration Methods . . . . . 6-11
Menu: Viewing and Configuring a Static Trunk Group . . . . . 6-15
Check the Event Log (page 11-10) to verify that the trunked ports are operating properly. . . . . 6-17
CLI: Viewing and Configuring a Static or Dynamic Port Trunk Group . . . . . 6-17
Using the CLI To View Port Trunks . . . . . 6-17
Using the CLI To Configure a Static or Dynamic Trunk Group . 6-19
Web: Viewing Existing Port Trunk Groups . . . . . 6-22
Trunk Group Operation Using LACP . . . . . 6-23
Default Port Operation . . . . . 6-24
LACP Notes and Restrictions . . . . . 6-25
Trunk Group Operation Using the “Trunk” Option . . . . . 6-26
Trunk Operation Using the “FEC” Option . . . . . 6-26

How the Switch Lists Trunk Data . . . . . 6-27
Outbound Traffic Distribution Across Trunked Links . . . . . 6-27

## 7 Using Passwords, Port Security, and Authorized IP Managers To Protect Against Unauthorized Access

**Using Password Security** . . . . . 7-2
Menu: Setting Manager and Operator passwords . . . . . 7-3
CLI: Setting Manager and Operator Passwords . . . . . 7-5
Web: Configuring User Names and Passwords . . . . . 7-6

**Configuring and Monitoring Port Security** . . . . . 7-7
Basic Operation . . . . . 7-7
Blocking Unauthorized Traffic . . . . . 7-8
Trunk Group Exclusion . . . . . 7-9
Planning Port Security . . . . . 7-9
CLI: Port Security Command Options and Operation . . . . . 7-11
CLI: Displaying Current Port Security Settings . . . . . 7-14
CLI: Configuring Port Security . . . . . 7-15
Web: Displaying and Configuring Port Security Features . . . . . 7-20
Reading Intrusion Alerts and Resetting Alert Flags . . . . . 7-20
Notice of Security Violations . . . . . 7-20
How the Intrusion Log Operates . . . . . 7-21
Keeping the Intrusion Log Current by Resetting Alert Flags . . . 7-21
Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags . . . . . 7-22
CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags . . . . . 7-23
Using the Event Log To Find Intrusion Alerts . . . . . 7-25
Web: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags . . . . . 7-26
Operating Notes for Port Security . . . . . 7-26

**Using IP Authorized Managers** . . . . . 7-28
Access Levels . . . . . 7-29
Defining Authorized Management Stations . . . . . 7-29
Overview of IP Mask Operation . . . . . 7-30
Menu: Viewing and Configuring IP Authorized Managers . . . . . 7-31
CLI: Viewing and Configuring Authorized IP Managers . . . . . 7-32
Listing the Switch's Current Authorized IP Manager(s) . . . . . 7-32
Configuring IP Authorized Managers for the Switch . . . . . 7-33

Web: Configuring IP Authorized Managers . . . . . 7-34
Building IP Masks . . . . . 7-34
Configuring One Station Per Authorized Manager IP Entry . . . . 7-34
Configuring Multiple Stations Per Authorized Manager IP Entry . . . . . 7-35
Additional Examples for Authorizing Multiple Stations . . . . . 7-37
Operating and Troubleshooting Notes . . . . . 7-37

## 8 Configuring for Network Management Applications

**SNMP Management Features** . . . . . 8-2

**Configuring for SNMP Access to the Switch** . . . . . 8-3

**SNMP Communities** . . . . . 8-5
Menu: Viewing and Configuring SNMP Communities . . . . . 8-5
To View, Edit, or Add SNMP Communities: . . . . . 8-5
CLI: Viewing and Configuring Community Names . . . . . 8-7
Listing Current Community Names and Values . . . . . 8-7
Configuring Identity Information . . . . . 8-8
Configuring Community Names and Values . . . . . 8-8

**Trap Receivers and Authentication Traps** . . . . . 8-9
CLI: Configuring and Displaying Trap Receivers . . . . . 8-10
Using the CLI To List Current SNMP Trap Receivers . . . . . 8-10
Configuring Trap Receivers . . . . . 8-11
Using the CLI To Enable Authentication Traps . . . . . 8-11

**Advanced Management: RMON Support** . . . . . 8-12
RMON . . . . . 8-12

## 9 Configuring Advanced Features

**Stack Management** . . . . . 9-2
Components of Stack Management . . . . . 9-4
General Stacking Operation . . . . . 9-4
Operating Rules for Stacking . . . . . 9-5
General Rules . . . . . 9-5
Specific Rules . . . . . 9-6
Overview of Configuring and Bringing Up a Stack . . . . . 9-8
General Steps for Creating a Stack . . . . . 9-10

Using the Menu Interface To View Stack Status And Configure Stacking . . . . . 9-12
Using the Menu Interface To View and Configure a Commander Switch . . . . . 9-12
Using the Menu To Manage a Candidate Switch . . . . . 9-14
Using the Commander To Manage The Stack . . . . . 9-16
Using the Commander To Access Member Switches for Configuration Changes and Monitoring Traffic . . . . . 9-23
Converting a Commander or Member to a Member of Another Stack . . . . . 9-24
Monitoring Stack Status . . . . . 9-25
Using the CLI To View Stack Status and Configure Stacking . . . . . 9-29
Using the CLI To View Stack Status . . . . . 9-31
Using the CLI To Configure a Commander Switch . . . . . 9-33
Adding to a Stack or Moving Switches Between Stacks . . . . . 9-35
Using the CLI To Remove a Member from a Stack . . . . . 9-40
Using the CLI To Access Member Switches for Configuration Changes and Traffic Monitoring . . . . . 9-42
SNMP Community Operation in a Stack . . . . . 9-44
Using the CLI To Disable or Re-Enable Stacking . . . . . 9-45
Transmission Interval . . . . . 9-45
Stacking Operation with Multiple VLANs Configured . . . . . 9-45
Web: Viewing and Configuring Stacking . . . . . 9-46
Status Messages . . . . . 9-47
**Port-Based Virtual LANs (Static VLANs)** . . . . . 9-48
Overview of Using VLANs . . . . . 9-51
VLAN Support and the Default VLAN . . . . . 9-51
Which VLAN Is Primary? . . . . . 9-51
Per-Port Static VLAN Configuration Options . . . . . 9-52
General Steps for Using VLANs . . . . . 9-54
Notes on Using VLANs . . . . . 9-54
Menu: Configuring VLAN Parameters . . . . . 9-55
To Change VLAN Support Settings . . . . . 9-55
Adding or Editing VLAN Names . . . . . 9-57
Adding or Changing a VLAN Port Assignment . . . . . 9-58
CLI: Configuring VLAN Parameters . . . . . 9-60
Web: Viewing and Configuring VLAN Parameters . . . . . 9-66
VLAN Tagging Information . . . . . 9-67

Effect of VLANs on Other Switch Features . . . . . 9-71
Spanning Tree Protocol Operation with VLANs . . . . . 9-71
IP Interfaces . . . . . 9-71
VLAN MAC Addresses . . . . . 9-72
Port Trunks . . . . . 9-72
Port Monitoring . . . . . 9-72
VLAN Restrictions . . . . . 9-73
Symptoms of Duplicate MAC Addresses in VLAN Environments . . . . . 9-73
**GVRP** . . . . . 9-74
General Operation . . . . . 9-75
Per-Port Options for Handling GVRP "Unknown VLANs" . . . . . 9-77
Per-Port Options for Dynamic VLAN Advertising and Joining . . . . . 9-79
GVRP and VLAN Access Control . . . . . 9-80
Port-Leave From a Dynamic VLAN . . . . . 9-80
Planning for GVRP Operation . . . . . 9-81
Configuring GVRP On a Switch . . . . . 9-81
Menu: Viewing and Configuring GVRP . . . . . 9-81
CLI: Viewing and Configuring GVRP . . . . . 9-83
Web: Viewing and Configuring GVRP . . . . . 9-86
GVRP Operating Notes . . . . . 9-86
**Multimedia Traffic Control with IP Multicast (IGMP)** . . . . . 9-88
IGMP Operating Features . . . . . 9-89
CLI: Configuring and Displaying IGMP . . . . . 9-90
Web: Enabling or Disabling IGMP . . . . . 9-94
How IGMP Operates . . . . . 9-94
Role of the Switch . . . . . 9-95
Number of IP Multicast Addresses Allowed . . . . . 9-98
**Spanning Tree Protocol (STP)** . . . . . 9-99
Menu: Configuring STP . . . . . 9-100
CLI: Configuring STP . . . . . 9-102
Web: Enabling or Disabling STP . . . . . 9-105
How STP Operates . . . . . 9-105
STP Fast Mode . . . . . 9-106
STP Operation with 802.1Q VLANs . . . . . 9-107

## 10 Monitoring and Analyzing Switch Operation

**Status and Counters Data** . . . . . 10-2

Menu Access To Status and Counters . . . . . 10-3
General System Information . . . . . 10-4
Menu Access . . . . . 10-4
CLI Access . . . . . 10-4
Switch Management Address Information . . . . . 10-5
Menu Access . . . . . 10-5
CLI Access . . . . . 10-5
Port Status . . . . . 10-6
Menu: Displaying Port Status . . . . . 10-6
CLI Access . . . . . 10-6
Web Access . . . . . 10-6
Viewing Port and Trunk Group Statistics . . . . . 10-7
Menu Access to Port and Trunk Statistics . . . . . 10-8
CLI Access To Port and Trunk Group Statistics . . . . . 10-9
Web Browser Access To View Port and Trunk Group Statistics 10-9
Viewing the Switch's MAC Address Tables . . . . . 10-10
Menu Access to the MAC Address Views and Searches . . . . . 10-11
CLI Access for MAC Address Views and Searches . . . . . 10-13
Spanning Tree Protocol (STP) Information . . . . . 10-14
Menu Access to STP Data . . . . . 10-14
CLI Access to STP Data . . . . . 10-15
Internet Group Management Protocol (IGMP) Status . . . . . 10-16
VLAN Information . . . . . 10-17
Web Browser Interface Status Information . . . . . 10-19
**Port Monitoring Features** . . . . . 10-20
Menu: Configuring Port Monitoring . . . . . 10-21
CLI: Configuring Port Monitoring . . . . . 10-23
Web: Configuring Port Monitoring . . . . . 10-25

## 11 Troubleshooting

**Troubleshooting Approaches** . . . . . 11-2
**Browser or Console Access Problems** . . . . . 11-3
**Unusual Network Activity** . . . . . 11-5
General Problems . . . . . 11-5
IGMP-Related Problems . . . . . 11-6
Problems Related to Spanning-Tree Protocol (STP) . . . . . 11-7
Stacking-Related Problems . . . . . 11-7
Timep or Gateway Problems . . . . . 11-7
VLAN-Related Problems . . . . . 11-8

**Using the Event Log To Identify Problem Sources** . . . . . 11-10
Menu: Entering and Navigating in the Event Log . . . . . 11-11
CLI: . . . . . 11-12

**Diagnostic Tools** . . . . . 11-13
Ping and Link Tests . . . . . 11-13
Web: Executing Ping or Link Tests . . . . . 11-14
CLI: Ping or Link Tests . . . . . 11-15
Displaying the Configuration File . . . . . 11-17
CLI: Viewing the Configuration File . . . . . 11-17
Web: Viewing the Configuration File . . . . . 11-17
CLI Administrative and Troubleshooting Commands . . . . . 11-18

**Restoring the Factory-Default Configuration** . . . . . 11-19
CLI: Resetting to the Factory-Default Configuration . . . . . 11-19
Clear/Reset: Resetting to the Factory-Default Configuration . 11-19

## A Transferring an Operating System or Startup Configuration File

**Downloading an Operating System (OS)** . . . . . A-1
Using TFTP To Download the OS File from a Server . . . . . A-2
Menu: TFTP Download from a Server . . . . . A-3
CLI: TFTP Download from a Server . . . . . A-4
Switch-to-Switch Download . . . . . A-4
Menu: Switch-to-Switch Download . . . . . A-4
CLI: Switch-To-Switch Download . . . . . A-5
Using Xmodem to Download the OS File From a PC . . . . . A-6
Menu: Xmodem Download . . . . . A-6
CLI: Xmodem Download from a PC or Unix Workstation . . . . . A-6

**Troubleshooting TFTP Downloads** . . . . . A-8

**Transferring Switch Configurations** . . . . . A-9

## B MAC Address Management

**Determining MAC Addresses** . . . . . B-1
Menu: Viewing the Switch's MAC Addresses . . . . . B-2
CLI: Viewing the Port and VLAN MAC Addresses . . . . . B-3

## C Switch Memory and Configuration

**Overview of Configuration File Management** . . . . . C-1

**Using the CLI To Implement Configuration Changes** . . . . . C-3

**Using the Menu and Web Browser Interfaces To Implement Configuration Changes** . . . . . C-6

Using the Menu Interface To Implement Configuration Changes . . C-6

Using Save and Cancel in the Menu Interface . . . . . C-7

Rebooting from the Menu Interface . . . . . C-8

Using the Web Browser Interface To Implement Configuration Changes . . . . . C-9

## D Daylight Savings Time

# Selecting a Management Interface

This chapter describes the following:

- Management interfaces for the SMC6624M switch
- Advantages of using each interface

## Understanding Management Interfaces

Management interfaces enable you to reconfigure the switch and to monitor switch status and performance. The SMC6624M switch offers the following interfaces:

- **Menu interface**—a menu-driven interface offering a subset of switch commands through the built-in VT-100/ANSI console—**page 1-2**
- **CLI**—a command line interface offering the full set of switch commands through the VT-100/ANSI console built into the switch—**page 1-3**
- **Web browser interface** –a switch interface offering status information and a subset of switch commands through a standard web browser (such as Netscape Navigator or Microsoft Internet Explorer)—**page 1-4**

This manual describes how to use the menu interface (chapter 2), the CLI (chapter 3), the web browser interface (chapter 4), and how to use these interfaces to configure and monitor the switch.

# Advantages of Using the Menu Interface

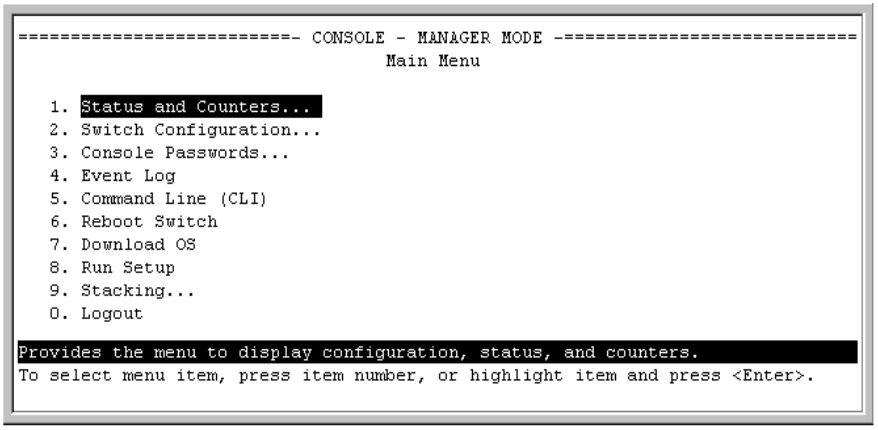



**Figure 1-1. Example of the Console Interface Display**

- **Provides quick, easy management access** to a menu-driven subset of switch configuration and performance features:

  - IP addressing
  - VLANs
  - Security
  - Port and Static Trunk Group
  - Stack Management
  - Spanning Tree
  - System information
  - Passwords and other security features
  - SNMP communities

  The menu interface also provides access for:

  - Setup screen
  - Event Log display
  - Switch and port status displays
  - Switch and port statistic and counter displays
  - Reboots
  - Software downloads

- **Offers out-of-band access** (through the RS-232 connection) to the switch, so network bottlenecks, crashes, lack of configured or correct IP address, and network downtime do not slow or prevent access.
- **Enables Telnet (in-band) access** to the menu functionality.
- **Allows faster navigation**, avoiding delays that occur with slower display of graphical objects over a web browser interface.
- **Provides more security**; configuration information and passwords are not seen on the network.

# Advantages of Using the CLI

| | |
|---|---|
| `SMC6624M>` | Operator Level |
| `SMC6624M#` | Manager Level |
| `SMC6624M(config)#` | Global Configuration Level |
| `SMC6624M(<context>)#` | Context Configuration Levels (port, VLAN) |

**Figure 1-2. Example of The Command Prompt**

- Provides access to the complete set of the switch configuration, performance, and diagnostic features.
- Offers out-of-band access (through the RS-232 connection) or Telnet (in-band) access.
- Enables quick, detailed system configuration and management access to system operators and administrators experienced in command prompt interfaces.
- Provides help at each level for determining available options and variables.

## CLI Usage

- For information on how to use the CLI, refer to chapter 3. “Using the Command Line Interface (CLI).”
- To perform specific procedures (such as configuring IP addressing or VLANs), use the Contents listing at the front of the manual to locate the information you need.
- To monitor and analyze switch operation, see chapter 10, “Monitoring and Analyzing Switch Operation.”
- For information on individual CLI commands, refer to the Index.

# Advantages of Using the Web Browser Interface

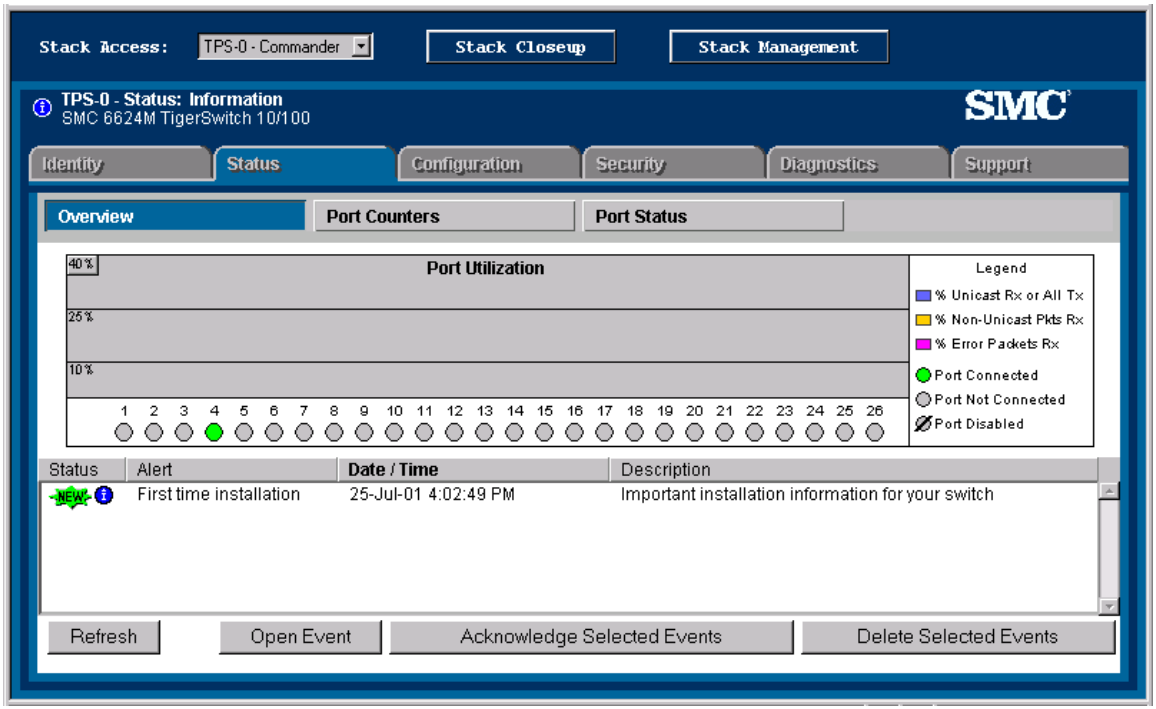



**Figure 1-3. Example of the Web Browser Interface**

- **Easy access** to the switch from anywhere on the network
- **Familiar browser interface**--locations of window objects consistent with commonly used browsers, uses mouse clicking for navigation, no terminal setup
- **Many features have all their fields in one scree**n so you can view all values at once
- **More visual cues**, using colors, status bars, device icons, and other graphical objects instead of relying solely on alphanumeric values
- **Display of acceptable ranges of values available** in configuration list boxes

For specific requirements, see “Web Browser Interface Requirements” on page 4-3.

# Using the Menu Interface

This chapter describes the following features:


- Overview of the Menu Interface (page 4-1)
- Starting and ending a Menu session (page 2-2)
- The Main Menu (page 2-6)
- Screen structure and navigation (page 2-8)
- Rebooting the switch (page 2-11)


The menu interface operates through the switch console to provide you with a subset of switch commands in an easy-to-use menu format enabling you to:

- Perform a "quick configuration" of basic parameters, such as the IP addressing needed to provide management access through your network
- Configure these features:
  - Manager and Operator passwords
  - System parameters
  - IP addressing
  - Ports
  - One trunk group
  - A network monitoring port
  - Stack Management
  - Spanning Tree operation
  - SNMP community names
  - IP authorized managers
  - VLANs (Virtual LANs)
- View status, counters, and Event Log information
- Download new software system
- Reboot the switch

For a detailed list of menu features, see the "Menu Features List" on page 2-13.

**Privilege Levels and Password Security.** SMC strongly recommends that you configure a Manager password to help prevent unauthorized access to your network. A Manager password grants full read-write access to the switch. An Operator password, if configured, grants access to status and counter, Event Log, and the Operator level in the CLI. After you configure passwords on the switch and log off of the interface, access to the menu interface (and the CLI and web browser interface) will require entry of either the Manager or Operator password. (If the switch has only a Manager password, then someone without a password can still gain read-only access.)

**Menu Interaction with Other Interfaces.**

- A configuration change made through any switch interface overwrites earlier changes made through any other interface.
- The Menu Interface and the CLI (Command Line Interface) both use the switch console. To enter the menu from the CLI, use the **menu** command. To enter the CLI from the Menu interface, select **Command Line (CLI)** option.)

# Starting and Ending a Menu Session



You can access the menu interface using any of the following:

- A direct serial connection to the switch's console port, as described in the installation guide you received with the switch
- A Telnet connection to the switch console from a networked PC or the switch's web browser interface. Telnet requires that an IP address and subnet mask compatible with your network have already been configured on the switch.
- The stack Commander, if the switch is a stack member

**Note**

This section assumes that either a terminal device is already configured and connected to the switch (see the *Installation Guide* shipped with your switch) or that you have already configured an IP address on the switch (required for Telnet access).

## How To Start a Menu Interface Session

In its factory default configuration, the switch console starts with the CLI prompt. To use the menu interface with Manager privileges, go to the Manager level prompt and enter the **menu** command.

1. Use one of these methods to connect to the switch:
   - A PC terminal emulator or terminal
   - Telnet

   (You can also use the stack Commander if the switch is a stack member. See "Stack Management" on page 9-2).

2. Do one of the following:
   - If you are using Telnet, go to step 3.
   - If you are using a PC terminal emulator or a terminal, press [Enter] one or more times until a prompt appears.

3. When the switch screen appears, do one of the following:
   - If a password has been configured, the password prompt appears.

     ```
     Password: _
     ```

     Type the Manager password and press [Enter]. Entering the Manager password gives you manager-level access to the switch. (Entering the Operator password gives you operator-level access to the switch. See "Using Password Security" on page 7-2.)
   - If no password has been configured, the CLI prompt appears. Go to the next step.

4. When the CLI prompt appears, display the Menu interface by entering the **menu** command. For example:

   ```
   SMC TigerSwitch 10/100# menu [Enter]
   ```

   results in:

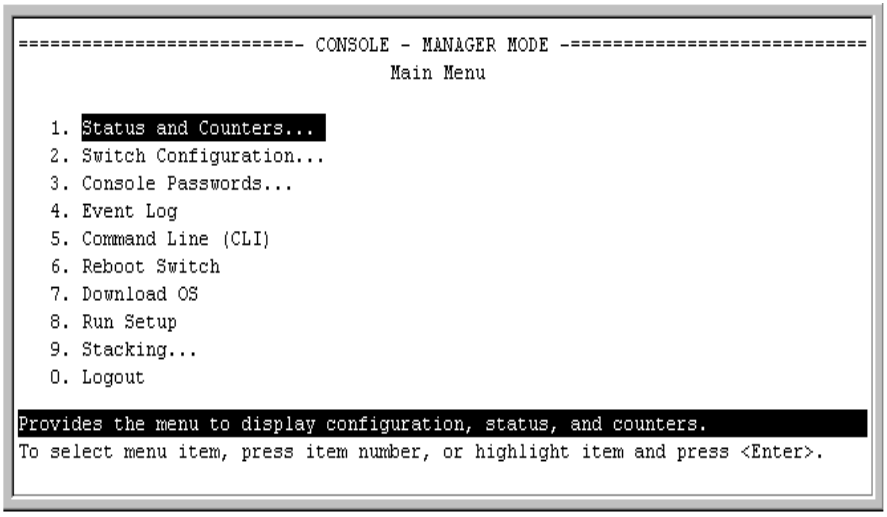



**Figure 2-1. The Main Menu with Manager Privileges**

For a description of Main Menu features, see "Main Menu Features" on page 2-6.

**Note**

To configure the switch to start with the menu interface instead of the CLI, go to the Manager level prompt, enter the **setup** command, and in the resulting desplay, change the **Logon Default** parameter to **Menu**. For more information, see the *Installation Guide* you received with the switch.

## How To End a Menu Session and Exit from the Console:

The method for ending a menu session and exiting from the console depends on whether, during the session, you made any changes to the switch configuration that require a switch reboot to activate. (Most changes need only a **Save**, and do not require a switch reboot.) Configuration changes needing a reboot are marked with an asterisk (*) next to the configured item in the Configuration menu and also next to the **Switch Configuration** item in the Main Menu.

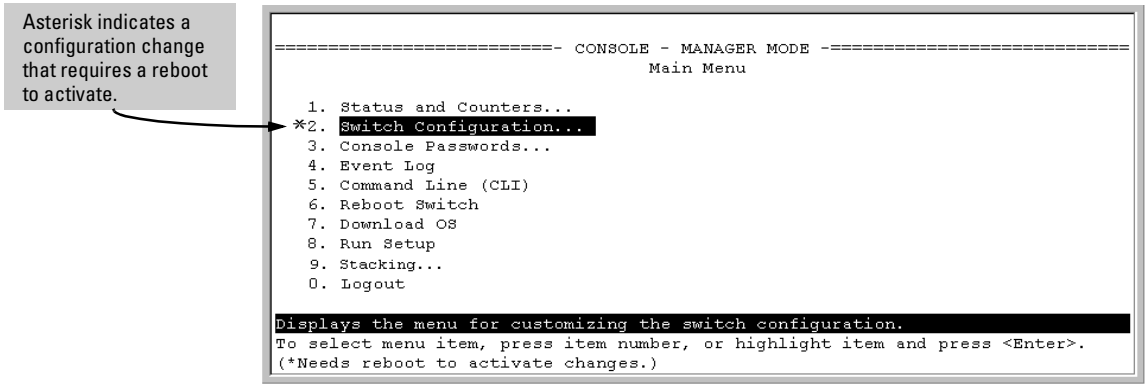



**Figure 2-2. An Asterisk Indicates a Configuration Change Requiring a Reboot**

1. In the current session, if you have not made configuration changes that require a switch reboot to activate, return to the Main menu and press [0] (zero) to log out. Then just exit from the terminal program, turn off the terminal, or quit the Telnet session.

2. If you *have* made configuration changes that require a switch reboot—that is, if an asterisk (*) appears next to a configured item or next to **Switch Configuration** in the Main menu:

   a. Return to the Main menu.

   b. Press [6] to select **Reboot Switch** and follow the instructions on the reboot screen.

   Rebooting the switch terminates the menu session, and, if you are using Telnet, disconnects the Telnet session.

   (See “Rebooting To Activate Configuration Changes” on page 2-12.)

3. Exit from the terminal program, turn off the terminal, or close the Telnet application program.

# Main Menu Features

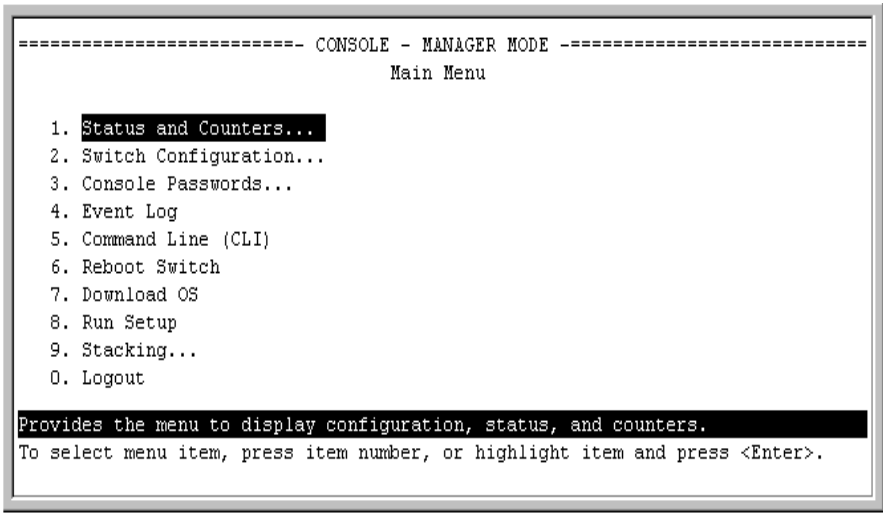



**Figure 2-3. The Main Menu View with Manager Privileges**

The Main Menu gives you access to these Menu interface features:

- **Status and Counters:** Provides access to display screens showing switch information, port status and counters, port and VLAN address tables, and spanning tree information. (See chapter 10, "Monitoring and Analyzing Switch Operation.")
- **Switch Configuration:** Provides access to configuration screens for displaying and changing the current configuration settings. (See the Contents listing at the front of this manual.) For a listing of features and parameters configurable through the menu interface, see the "Menu Features List" on page 2-13.
- **Console Passwords:** Provides access to the screen used to set or change Manager-level and Operator-level passwords, and to delete Manager and Operator password protection. (See "Using Password Security" on page page 7-2.)
- **Event Log:** Enables you to read progress and error messages that are useful for checking and troubleshooting switch operation. (See "Using the Event Log To Identify Problem Sources" on page 11-10.)

- **Command Line (CLI):** Selects the Command Line Interface at the same level (Manager or Operator) that you are accessing in the Menu interface. (See chapter 3, "Using the Command Line Interface (CLI).")
- **Reboot Switch:** Performs a "warm" reboot of the switch, which clears most temporary error conditions, resets the network activity counters to zero, and resets the system up time to zero. A reboot is required to activate a change in the VLAN Support parameter. (See "Rebooting from the Menu Interface" on page C-8.)
- **Download OS:** Enables you to download a new software version to the switch. (See appendix A, "Transferring an Operating System or Configuration.")
- **Run Setup:** Displays the Switch Setup screen for quickly configuring basic switch parameters such as IP addressing, default gateway, logon default interface, spanning tree, and others. (See the *Installation Guide* shipped with your switch.)
- **Stacking:** Enables you to use a single IP address and standard network cabling to manage a group of up to 16 switches in the same subnet (broadcast domain). See "Stack Management" on page 9-2.
- **Logout:** Closes the Menu interface and console session, and disconnects Telnet access to the switch. (See "How to End a Menu Session and Exit from the Console" on page 2-4.)

# Screen Structure and Navigation

Menu interface screens include these three elements:

- Parameter fields and/or read-only information such as statistics
- Navigation and configuration actions, such as Save, Edit, and Cancel
- Help line to describe navigation options, individual parameters, and read-only data

For example, in the following System Information screen:

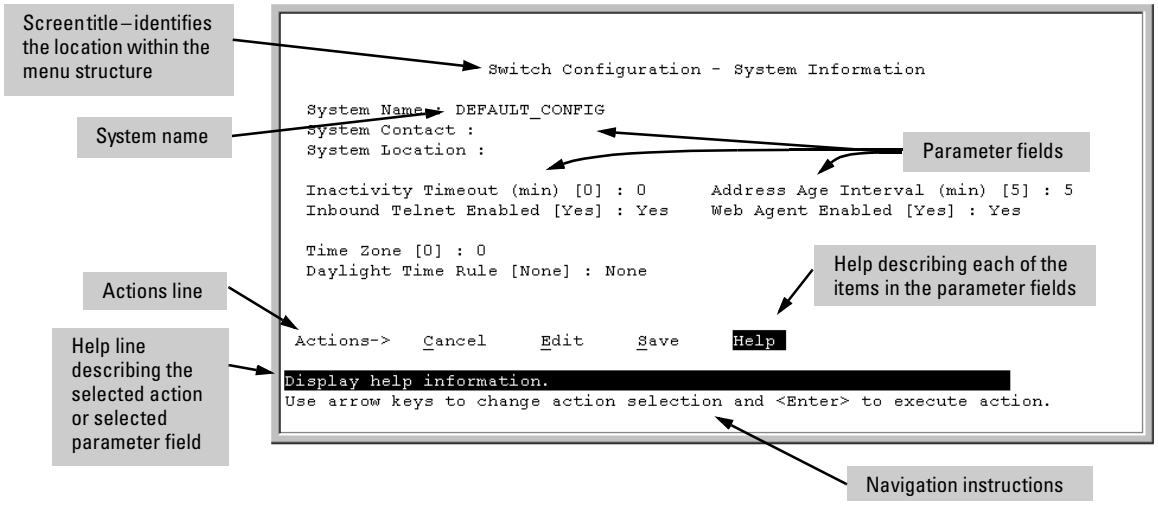



**Figure 4-1. Elements of the Screen Structure**

**"Forms" Design**. The configuration screens, in particular, operate similarly to a number of PC applications that use forms for data entry. When you first enter these screens, you see the current configuration for the item you have selected. To change the configuration, the basic operation is to:

1. Press [E] to select the **Edit** action.
2. Navigate through the screen making all the necessary configuration changes. (See Table 4-1 on the next page.)
3. Press [Enter] to return to the **Actions** line. From there you can save the configuration changes or cancel the changes. Cancel returns the configuration to the values you saw when you first entered the screen.

**Table 4-1. How To Navigate in the Menu Interface**

| Task: | Actions: |
|---|---|
| Execute an action from the "Actions –>" list at the bottom of the screen: | Use either of the following methods:<br>• Use the arrow keys ( ← ,or → ) to highlight the action you want to execute, then press [Enter].<br>• Press the key corresponding to the capital letter in the action name. For example, in a configuration menu, press [E] to select Edit and begin editing parameter values. |
| Reconfigure (edit) a parameter setting or a field: | 1. Select a configuration item, such as **System Name**. (See figure 4-1.)<br>2. Press [E] (for **Edit** on the Actions line).<br>3. Use [Tab] or the arrow keys (←, →, ↑, or ↓) to highlight the item or field.<br>4. Do one of the following:<br>– If the parameter has preconfigured values, either use the Space bar to select a new option or type the first part of your selection and the rest of the selection appears automatically. (The help line instructs you to "Select" a value.)<br>– If there are no preconfigured values, type in a value (the Help line instructs you to "Enter" a value).<br>5. If you want to change another parameter value, return to step 3.<br>6. If you are finished editing parameters in the displayed screen, press [Enter] to return to the Actions line and do one of the following:<br>– To save and activate configuration changes, press [S] (for the **Save** action). This saves the changes in the startup configuration and also implements the change in the currently running configuration. (See appendix C, "Switch Memory and Configuration.)<br>– To exit from the screen without saving any changes that you have made (or if you have not made changes), press [C] (for the **Cancel** action).<br>***Note:*** In the menu interface, executing Save activates most parameter changes and saves them in the startup configuration (or flash) memory, and it is therefore not necessary to reboot the switch after making these changes. But if an asterisk appears next to any menu item you reconfigure, the switch will not activate or save the change for that item until you reboot the switch. In this case, rebooting should be done after you have made all desired changes and then returned to the Main Menu.<br>7. When you finish editing parameters, return to the Main Menu.<br>8. If necessary, reboot the switch by highlighting Reboot Switch in the Main Menu and pressing [Enter]. (See the ***Note***, above.) |
| Exit from a read-only screen. | Press [B] (for the **Back** action). |

**To get Help on individual parameter descriptions.** In most screens there is a **Help** option in the **Actions** line. Whenever any of the items in the **Actions** line is highlighted, press [H], and a separate help screen is displayed. For example:

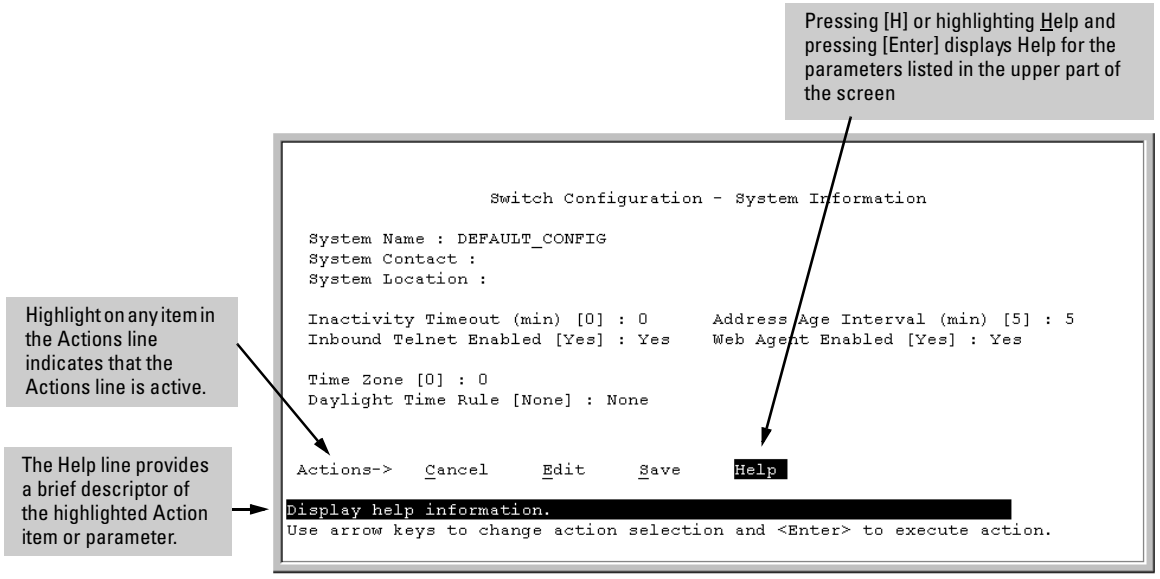



**Figure 4-2. Example Showing How To Display Help**

**To get Help on the actions or data fields in each screen:** Use the arrow keys ( ←, →, ↑, or ↓) to select an action or data field. The help line under the **Actions** items describes the currently selected action or data field.

**For guidance on how to navigate in a screen:** See the instructions provided at the bottom of the screen, or refer to "Screen Structure and Navigation" on page 2-8.)

# Rebooting the Switch

Rebooting the switch from the menu interface

- Terminates all current sessions and performs a reset of the operating system
- Activates any configuration changes that require a reboot
- Resets statistical counters to zero

(Note that statistical counters can be reset to zero without rebooting the switch.)

To Reboot the switch, use the **Reboot Switch** option in the Main Menu. (Note that the Reboot Switch option is not available if you log on in Operator mode; that is, if you enter an Operator password instead of a manager password at the password prompt.)

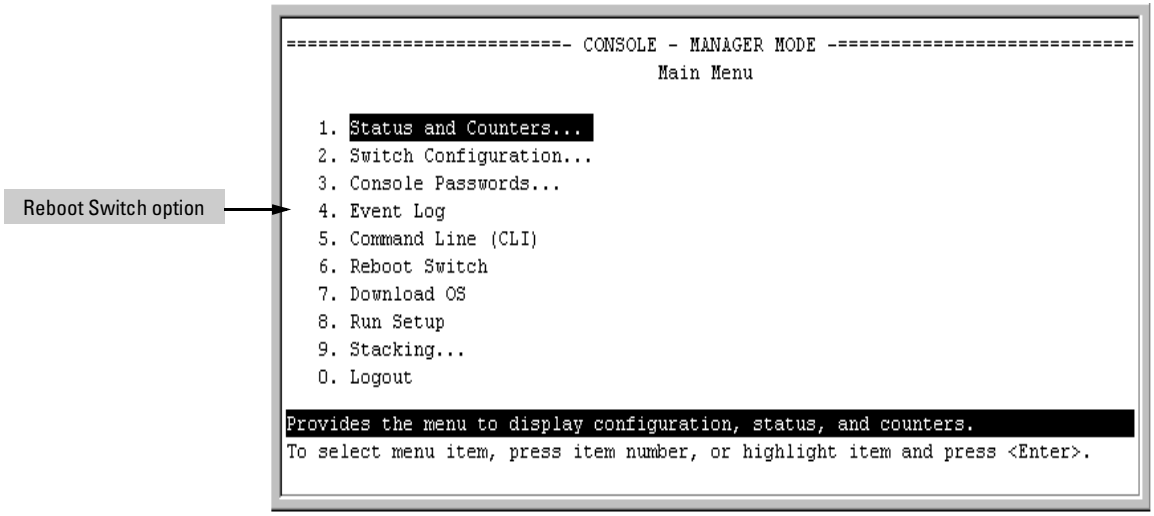



**Figure 4-3. The Reboot Switch Option in the Main Menu**

**Rebooting To Activate Configuration Changes.** Configuration changes for most parameters become effective as soon as you save them. However, you must reboot the switch in order to implement a change in the **Maximum VLANs to support parameter**. (To access this parameter, go to the Main menu and select **2. Switch Configuration**, then **8. VLAN Menu**, then **1. VLAN Support**.)

If configuration changes requiring a reboot have been made, the switch displays an asterisk (*) next to the menu item in which the change has been made. For example, if you change and save the value for the **Maximum VLANs to support** parameter, an asterisk appears next to the **VLAN Support** entry in the VLAN Menu screen, and also next to the the **Switch Configuration . . .** entry in the Main menu, as shown in figure 4-6:

Asterisk indicates a configuration change that requires a reboot in order to take effect.

Reminder to reboot the switch to activate configuration changes.

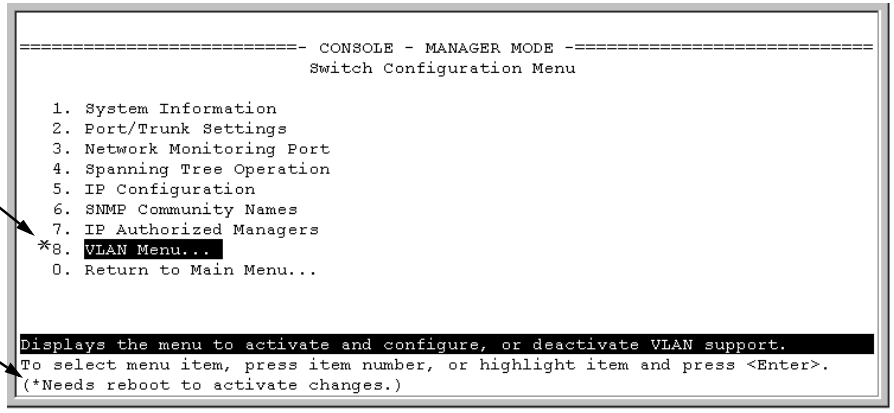



**Figure 4-4. Indication of a Configuration Change Requiring a Reboot**

To activate changes indicated by the asterisk, go to the Main Menu and select the **Reboot Switch** option.

**Note**

Executing the **write memory** command in the CLI does not affect pending configuration changes indicated by an asterisk in the menu interface. That is, only a reboot from the menu interface or a boot or reload command from the CLI will activate a pending configuration change indicated by an asterisk.

# Menu Features List

Status and Counters

- General System Information
- Switch Management Address Information
- Port Status
- Port Counters
- Address Table
- Port Address Table
- Spanning Tree Information

Switch Configuration

- System Information
- Port/Trunk Settings
- Network Monitoring Port
- Spanning Tree Operation
- IP Configuration
- SNMP Community Names
- IP authorized Managers
- VLAN Menu

Console Passwords

Event Log

Command Line (CLI)

Reboot Switch

Download OS

Run Setup

Stacking

- Stacking Status (This Switch)
- Stacking Status (All)
- Stack Configuration
- Stack Management *(Available in Stack Commander Only)*
- Stack Access *(Available in Stack Commander Only)*

Logout

# Where To Go From Here

This chapter provides an overview of the menu interface and how to use it. The following table indicates where to turn for detailed information on how to use the individual features available through the menu interface.

| Option | Where To Turn |
|---|---|
| To use the Run Setup option | See the Installation Guide shipped with the switch. |
| To use the Stack Manager | "Stack Management" on page 9-2 |
| To view and monitor switch status and counters | Chapter 10, "Monitoring and Analyzing Switch Operation" |
| To learn how to configure and use passwords | "Using Password Security" on page 7-2 |
| To learn how to use the Event Log | "Using the Event Log To Identify Problem Sources" on page 11-10 |
| To learn how the CLI operates | Chapter 3, "Using the Command Line Interface (CLI)" |
| To download software (the OS) | Appendix A, "File Transfers" |
| For a description of how switch memory handles configuration changes | Appendix C, "Switch Memory and Configuration" |
| For information on other switch features and how to configure them | See the Table of Contents at the front of this manual. |

# Using the Command Line Interface (CLI)

The CLI is a text-based command interface for configuring and monitoring the switch. The CLI gives you access to the switch's full set of commands while providing the same password protection that is used in the web browser interface and the menu interface.

## Accessing the CLI

Like the menu interface, the CLI is accessed through the switch console, and, in the switch's factory default state, is the default interface when you start a console session. You can access the console out-of-band by directly connecting a terminal device to the switch, or in-band by using Telnet either from a terminal device or through the web browser interface.

Also, if you are using the menu interface, you can access the CLI by selecting the **Command Line (CLI)** option in the Main Menu.

## Using the CLI

The CLI offers these privilege levels to help protect the switch from unauthorized access:

- Operator
- Manager
- Global Configuration
- Context Configuration

**Note** CLI commands are not case-sensitive.

When you use the CLI to make a configuration change, the switch writes the change to the Running-Config file in volatile memory. This allows you to test your configuration changes before making them permanent. to make changes permanent, you must use the **write memory** command to save them to the Startup Config file in non-volatile memory. If you reboot the switch without first using **write memory**, all changes made since the last reboot or **write memory** (whichever is later) will be lost. For more on switch memory and saving configuration changes, see appendix C, "Switch Memory and Configuration."

## Privilege Levels at Logon

Privilege levels control the type of access to the CLI. To implement this control, you must set at least a Manager password. *Without a Manager password configured, anyone having serial port, Telnet, or web browser access to the switch can reach all CLI levels.* (For more on setting passwords, see "Using Password Security" on page 7-2.)

When you use the CLI to log on to the switch, and passwords are set, you will be prompted to enter a password. For example:

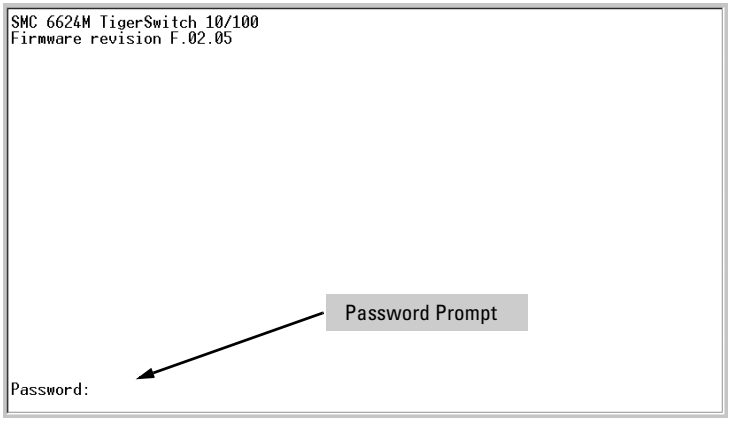



**Figure 3-1. Example of CLI Log-On Screen with Password(s) Set**

In the above case, you will enter the CLI at the level corresponding to the password you provide (operator or manager).

If no passwords are set when you log onto the CLI, you will enter at the Manager level. For example:

```
SMC TigerSwitch 10/100# _
```

**Caution**

SMC strongly recommends that you configure a Manager password. If a Manager password is not configured, then the Manager level is not password-protected, and anyone having in-band or out-of-band access to the switch may be able to reach the Manager level and compromise switch and network security. Note that configuring only an Operator password *does not* prevent access to the Manager level by intruders who have the Operator password.

Pressing the Clear button on the front of the switch removes password protection. *For this reason, it is recommended that you protect the switch from physical access by unauthorized persons*. If you are concerned about switch security and operation, you should install the switch in a secure location, such as a locked wiring closet.

## Privilege Level Operation

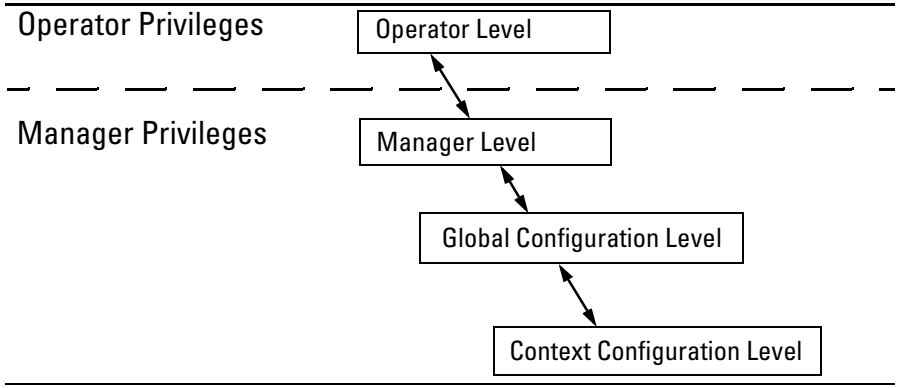



**Figure 3-2. Privilege Level Access Sequence**

### Operator Privileges

At the Operator level you can examine the current configuration and move between interfaces without being able to change the configuration. A ">" character delimits the Operator-level prompt. For example:

```
SMC TigerSwitch 10/100> _
```
(Example of the Operator prompt.)

When using **enable** to move to the Manager level, the switch prompts you for the Manager password if one has already been configured.

## Manager Privileges

Manager privileges give you three additional levels of access: Manager, Global Configuration, and Context Configuration. (See figure .) A "#" character delimits any Manager prompt. For example:

`SMC TigerSwitch 10/100#_` (Example of the Manager prompt.)

- **Manager level**: Provides all Operator level privileges plus the ability to perform system-level actions that do not require saving changes to the system configuration file. The prompt for the Manager level contains only the system name and the "#" delimiter, as shown above. To select this level, enter the **enable** command at the Operator level prompt and enter the Manager password, when prompted. For example:

  ```
  SMC TigerSwitch 10/100> enable
  (Enter enable at the Operator prompt.)
  SMC TigerSwitch 10/100# _      (The Manager prompt.)
  ```

- **Global Configuration level:** Provides all Operator and Manager level privileges, and enables you to make configuration changes to any of the switch's software features. The prompt for the Global Configuration level includes the system name and "`(config).`" To select this level, enter the **config** command at the Manager prompt. For example:

  ```
  SMC TigerSwitch 10/100# _
  (Enter config at the Manager prompt.)
  SMC TigerSwitch 10/100(config)#_
  (The Global Config prompt.)
  ```

- **Context Configuration level:** Provides all Operator and Manager privileges, and enables you to make configuration changes in a specific context, such as one or more ports or a VLAN. The prompt for the Context Configuration level includes the system name and the selected context. For example:

  ```
  SMC TigerSwitch 10/100(eth-1)#

  SMC TigerSwitch 10/100(vlan-10)#
  ```

  The Context level is useful, for example, if you want to execute several commands directed at the same port or VLAN, or if you want to shorten the command strings for a specific context area. To select this level, enter the specific context at the Global Configuration level prompt. For example, to select the context level for an existing VLAN with the VLAN ID of 10, you would enter the following command and see the indicated result:

  ```
  SMC TigerSwitch 10/100(config)# vlan 10
  ```

```
SMC TigerSwitch 10/100(vlan-10)#
```

**Changing Interfaces.** If you change from the CLI to the menu interface, or the reverse, you will remain at the same privilege level. For example, entering the `menu` command from the Operator level of the CLI takes you to the Operator privilege level in the menu interface.

**Table 3-1. Privilege Level Hierarchy**

| Privilege Level | Example of Prompt and Permitted Operations | | |
|---|---|---|---|
| **Operator Privilege** | | | |
| Operator Level | **SMC TigerSwitch 10/100>** | **show *<command>*** | View status and configuration information. |
| | | **setup** | |
| | | **ping *<argument>*** | Perform connectivity tests. |
| | | **link-test *<argument>*** | |
| | | **enable** | Move from the Operator level to the Manager level. |
| | | **menu** | Move from the CLI interface to the menu interface. |
| | | **logoff** | Exit from the CLI interface and terminate the console session. |
| **Manager Privilige** | | | |
| Manager Level | **SMC TigerSwitch 10/100#** | Perform system-level actions such as system control, monitoring, and diagnostic commands, plus any of the Operator-level commands. For a list of available commands, enter **?** at the prompt. | |
| Global Configuration Level | **SMC TigerSwitch 10/100(config)#** | Execute configuration commands, plus all Operator and Manager commands . For a list of available commands, enter **?** at the prompt. | |
| Context Configuration Level | **SMC TigerSwitch 10/100(eth-5)#**<br>**SMC TigerSwitch 10/100(vlan-100)#** | Execute context-specific configuration commands, such as a particular VLAN or switch port. This is useful for shortening the command strings you type, and for entering a series of commands for the same context. For a list of available commands, enter **?** at the prompt. | |

## How To Move Between Levels

| Change in Levels | Example of Prompt , Command, and Result |
|---|---|
| Operator level<br>*to*<br>Manager level | `SMC TigerSwitch 10/100> enable`<br>`Password:_`<br>After you enter **enable**, the Password prompt appears. After you enter the Manager password, this prompt appears:<br>`SMC TigerSwitch 10/100#_` |
| Manager level<br>*to*<br>Global configuration level | `SMC TigerSwitch 10/100# config`<br>`SMC TigerSwitch 10/100(config)#` |
| Global configuration level<br>*to a*<br>Context configuration level | `SMC TigerSwitch 10/100(config)# vlan-10`<br>`SMC TigerSwitch 10/100(vlan-10)#` |
| Context configuration level<br>*to another*<br>Context configuration level | `SMC TigerSwitch 10/100(vlan-10)# interface ethernet 3`<br>`SMC TigerSwitch 10/100(int-3)#` |
| Move from any level to the preceding level | `SMC TigerSwitch 10/100(int-3)# exit`<br>`SMC TigerSwitch 10/100(config)# exit`<br>`SMC TigerSwitch 10/1002# exit`<br>`SMC TigerSwitch 10/1002>` |
| Move from any level to the Manager level | `SMC TigerSwitch 10/100(int-3)# end`<br>`SMC TigerSwitch 10/100#`<br>*—or—*<br>`SMC TigerSwitch 10/100(config)# end`<br>`SMC TigerSwitch 10/100#` |

**Moving Between the CLI and the Menu Interface.** When moving between interfaces, the switch retains the current privilege level (Manager or Operator). That is, if you are at the Operator level in the menu and select the **Command Line Interface (CLI)** option from the Main Menu, the CLI prompt appears at the Operator level.

**Changing Parameter Settings.** Regardless of which interface is used (CLI, menu interface, or web browser interface), the most recently configured version of a parameter setting overrides any earlier settings for that parameter.

For example, if you use the CLI to set a Manager password, and then later use the Setup screen (in the menu interface) to set a different Manager password, then the first password will be replaced by the second one.

## Listing Commands and Command Options

At any privilege level you can:

- List all of the commands available at that level
- List the options for a specific command

### Listing Commands Available at Any Privilege Level

At a given privilege level you can execute the commands that level offers, plus all of the commands available at preceding levels. Similarly, at a given privilege level, you can list all of that level's commands plus the commands made available at preceding levels. For example, at the Operator level, you can list and execute only the Operator level commands. However, at the Manager level, you can list and execute the commands available at both the Operator and Manager levels.

**Type "?" To List Available Commands.** Typing the **?** symbol lists the commands you can execute at the current privilege level. For example, typing **?** at the Operator level produces this listing:

```
SMC TigerSwitch 10/100> ?

 enable                Enter the Manager Exec context
 exit                  Return to the previous context or terminate current
                       session if in the outermost context
 link-test             Test the connection to a MAC address on the LAN
 logout                Terminate this console/telnet session
 menu                  Switch to the menu system
 ping                  Send IP Ping requests to a device on the network
 show                  Display configuration and status/counter information
SMC TigerSwitch 10/100>
```

**Figure 3-3. Example of the Operator Level Command Listing**

Typing **?** at the Manager level produces this listing:

```
SMC TigerSwitch 10/100# ?

 boot                  Reboot the device
 configure             Enter the Configuration context
 copy                  Copy datafiles to/from the switch
 end                   Return to the Manager Exec context
 erase                 Erase configuration file stored in flash
 getMIB                Retrieve and display the MIB objects specified
 kill                  Kill all other active telnet/console sessions
 log                   Display log events
 page                  Toggle paging mode
 print                 Execute command and redirect its output
 redo                  Re-execute a command from history
 reload                Warm reboot of the switch
 repeat                Repeat execution of the previous command
 clear                 Reset sundry statistics
 setMIB                Set the value of a MIB object
 setup                 Set up initial configuration for the switch
 telnet                Initiate an outbound telnet session
 terminal              Set the dimensions of the terminal window
 update                Enter ROM monitoring mode
 walkMIB               Display MIB objects and values
 write                 View or save the running configuration of the switch
-- MORE --
```

When - - MORE - - appears, use the Space bar or [Return] to list additional commands.

**Figure 3-4. Example of the Manager-Level Command Listing**

When **- - MORE - -** appears, there are more commands in the listing. To list the next screenfull of commands, press the Space bar. To list the remaining commands one-by-one, repeatedly press [Enter].

Typing **?** at the Global Configuration level or the Context Configuration level produces similar results.

**Use [Tab] To Search for or Complete a Command Word.** You can use [Tab] to help you find CLI commands or to quickly complete the current word in a command. To do so, press [Tab] immediately after typing the last letter of the last keyword in the CLI (with no spaces allowed). For example, at the Global Configuration level, if you press [Tab] immediately after typing "**t**," the CLI displays the available command options that begin with "t." For example:

```
SMC TigerSwitch 10/100(config)# t[Tab]
telnet-server
time
trunk
telnet
SMC TigerSwitch 10/100(config)# t
```

As mentioned above, if you type part of a command word and press [Tab], the CLI completes the current word (if you have typed enough of the word for the CLI to distinguish it from other possibilities), including hyphenated extensions. For example:

```
SMC TigerSwitch 10/100(config)# port[Tab]
SMC TigerSwitch 10/100(config)# port-security _
```

Pressing [Tab] after a completed command word lists the further options for that command.

```
SMC TigerSwitch 10/100(config)# stack[Tab]
 commander <commander-str>
 join <mac-addr>
 auto-join
 transmission-interval <integer>
 <cr>
SMC TigerSwitch 10/100(config)# stack
```

## Command Option Displays

**Conventions for Command Option Displays.** When you use the CLI to list options for a particular command, you will see one or more of the following conventions to help you interpret the command data:

- Braces ( < > ) indicate a required choice.
- Square brackets ( [ ] ) indicate optional elements.
- Vertical bars ( | ) separate alternative, mutually exclusive options in a command.

```
SMC TigerSwitch 10/100(config)# trunk?
 <trk1>
 <trunk|lacp>
 <[ethernet] port-list>
SMC TigerSwitch 10/100(config)# trunk
```

The braces (**< >**) show that the trunk command requires all three parameters.

The vertical bar ( **|** ) shows that either **trunk** or **lacp** must be included.

The square brackets (**[ ]**) show that **ethernet** is optional.

**Figure 3-5.Example of Command Option Conventions**

Thus, if you wanted to create a port trunk group using ports 5 - 8, the above conventions show that you could do so using any of the following forms of the **trunk** command:

```
SMC TigerSwitch 10/100(config)# trunk trk1 trunk 5-8
SMC TigerSwitch 10/100(config)# trunk trk1 trunk e 5-8

SMC TigerSwitch 10/100(config)# trunk trk1 lacp 5-8
SMC TigerSwitch 10/100(config)# trunk trk1 lacp e 5-8
```

**Listing Command Options.** You can use the CLI to remind you of the options available for a command by entering command keywords followed by **?**. For example, suppose you wanted to see the command options for configuring port 5:

```
SMC TigerSwitch 10/100(config)# interface e 5?
 flow-control          Enable/disable flow control on the port
 speed-duplex          Define mode of operation for the port
 broadcast-limit       Set a broadcast traffic percentage limit
 unknown-vlans         Define what the port will do when it encounters GVRP
                       packet requesting it to join a VLAN
 enable                Enable port
 disable               Disable port
 lacp                  Define whether LACP is enabled on the port, and whether
                       it is in active or passive mode when enabled

 monitor               Define that the port is to be monitored
 <cr>
```

This example displays the command options for configuring port 5 on the switch.

**Figure 3-6. Example of How To List the Options for a Specific Command**

## Displaying CLI "Help"

CLI Help provides two types of context-sensitive information:

- Command list with a brief summary of each command's purpose
- Detailed information on how to use individual commands

**Displaying Command-List Help.** You can display a listing of command Help summaries for all commands available at the current privilege level. That is, when you are at the Operator level, you can display the Help summaries only for Operator-Level commands. At the Manager level, you can display the Help summaries for both the Operator and Manager levels, and so on.

***Syntax:*** **help**

For example, to list the Operator-Level commands with their purposes:

```
SMC TigerSwitch 10/100> help
 enable             Enter the Manager Exec context.
 exit               Return to the previous context or terminate current
                    session if in the outermost context.
 link-test          Test the connection to a MAC address on the LAN.
 logout             Terminate this console/telnet session.
 menu               Switch to the menu system.
 ping               Send IP Ping requests to a device on the network.
 show               Display configuration and status/counter information.
```

**Figure 3-7. Example of Context-Sensitive Command-List Help**

**Displaying Help for an Individual Command.** You can display Help for any command that is available at the current context level by entering enough of the command string to identify the command, along with help.

**Syntax:** ***<command string>*** **help**

For example, to list the Help for the **interface** command in the Global Configuration privilege level:

```
SMC TigerSwitch 10/100(config)# interface help
Usage: interface ethernet <port-list>
       interface ethernet <port-list> commands

Description: Enter the Interface Configuration Level, or execute one
             command on that level.
             The first version of this command moves the switches
             current working level to the Interface Configuration Level
             using port-list for the current context. Commands that are
             subsequently invoked at this level apply to the port-list
             specified when entering the level. The second version of
             this command does not enter the Interface Configuration
             Level but does apply the 'commands' specified to the
             port-list. Valid 'commands' at this level include all
             commands available at the Interface Configuration Level.
```

**Figure 3-8. Example of How To Display Help for a Specific Command**

A similar action lists the Help showing additional parameter options for a given command. The following example illustrates how to list the Help for an interface command acting on a specific port:

```
SMC TigerSwitch 10/100(config)# interface e 5 help
 flow-control       Enable/disable flow control on the port.
 speed-duplex       Define mode of operation for the port.
 broadcast-limit    Set a broadcast traffic percentage limit.
 unknown-vlans      Define what the port will do when it encounters GVRP
                    packet requesting it to join a VLAN.
 enable             Enable port.
 disable            Disable port.
 lacp               Define whether LACP is enabled on the port, and whether it
                    is in active or passive mode when enabled.
 monitor            Define that the port is to be monitored.
```

**Figure 3-9. Example of Help for a Specific Instance of a Command**

Note that if you try to list the help for an individual command from a privilege level that does not include that command, the switch returns an error message. For example, trying to list the help for the interface command while at the global configuration level produces this result:

```
SMC TigerSwitch 10/100# interface help
Invalid input: interface
```



## Configuration Commands and the Context Configuration Modes

You can execute any configuration command in the global configuration mode or in selected context modes. However, using a context mode enables you to execute context-specific commands faster, with shorter command strings.

The SMC6624M offers interface (port or trunk group) and VLAN context configuration modes:

**Port or Trunk-Group Context .** Includes port- or trunk-specific commands that apply only to the selected port(s) or trunk group, plus the global configuration, Manager, and Operator commands. The prompt for this mode includes the identity of the selected port(s):

| | |
|---|---|
| `SMC TigerSwitch 10/100(config)# interface e 5-8` | Command executed at configuration level for entering port or trk1 static trunk-group context. |
| `SMC TigerSwitch 10/100(config)# interface e trk1` | |
| `SMC TigerSwitch 10/100(eth-5-8)#`<br>`SMC TigerSwitch 10/100(eth-Trk1)#` | Resulting prompt showing port or static trunk contexts. |

```
SMC TigerSwitch 10/100(eth-5-8)# ?
```

Lists the commands you can use in the port or static trunk context, plus the Manager, Operator, and context commands you can execute at this level.

```
SMC TigerSwitch 10/100(eth-5-8)# ?

 flow-control        Enable/disable flow control on the port
 speed-duplex        Define mode of operation for the port
 broadcast-limit     Set a broadcast traffic percentage limit
 unknown-vlans       Define what the port will do when it encounters GVRP
                     packet requesting it to join a VLAN
 enable              Enable port
 disable             Disable port
 lacp                Define whether LACP is enabled on the port, and whether
                     it is in active or passive mode when enabled
 monitor             Define that the port is to be monitored

 interface           Enter the Interface Configuration Level, or execute one
                     command on that level
 vlan                Add, delete, edit VLAN configuration or enter a VLAN
                     context

 boot                Reboot the device
 configure           Enter the Configuration context
 copy                Copy datafiles to/from the switch
 end                 Return to the Manager Exec context
 erase               Erase configuration file stored in flash
-- MORE --
```

In the port context, the first block of commands in the "?" listing show the context-specific commands that will affect only ports 5-8.

The remaining commands in the listing are Manager, Operator, and context commands.

**Figure 3-10. Context-Specific Commands Affecting Port Context**

**VLAN Context.** Includes VLAN-specific commands that apply only to the selected VLAN, plus Manager and Operator commands. The prompt for this mode includes the VLAN ID of the selected VLAN. For example, if you had already configured a VLAN with an ID of 100 in the switch:

| | |
|---|---|
| `SMC TigerSwitch 10/100(config)# vlan 100` | Command executed at configuration level to enter VLAN 100 context. |
| `SMC TigerSwitch 10/100(vlan-100)#` | Resulting prompt showing VLAN 100 context. |
| `SMC TigerSwitch 10/100(vlan-100)# ?` | Lists commands you can use in the VLAN context, plus Manager, Operator, and context commands you can execute at this level. |



In the VLAN context, the first block of commands in the "?" listing show the commands that will affect only vlan-100.

The remaining commands in the listing are Manager, Operator, and context commands.

```
SMC TigerSwitch 10/100(vlan-100)# ?

  ip                    Configures IP parameters for a VLAN
  monitor               Define that the VLAN is to be monitore
  name                  Set the VLAN's name
  tagged                Assign ports to current VLAN as tagged
  forbid                Prevents ports from becoming a member
                        VLAN
  untagged              Assign ports to current VLAN as untagg

  interface             Enter the Interface Configuration Leve
                        command on that level
  vlan                  Add, delete, edit VLAN configuration o
                        context

  boot                  Reboot the device
  configure             Enter the Configuration context
  copy                  Copy datafiles to/from the switch
  end                   Return to the Manager Exec context
  erase                 Erase configuration file stored in fla
  getMIB                Retrieve and display the MIB objects s
  kill                  Kill all other active telnet/console s
  log                   Display log events
 -- MORE --
```

**Figure 3-11. Context-Specific Commands Affecting VLAN Context**

# CLI Control and Editing

| Keystrokes | Function |
|---|---|
| [Ctrl] [A] | Jumps to the first character of the command line. |
| [Ctrl] [B] or ← | Moves the cursor back one character. |
| [Ctrl] [C] | Terminates a task and displays the command prompt. |
| [Ctrl] [D] | Deletes the character at the cursor. |
| [Ctrl] [E] | Jumps to the end of the current command line. |
| [Ctrl] [F] or → | Moves the cursor forward one character. |
| [Ctrl] [K] | Deletes from the cursor to the end of the command line. |
| [Ctrl] [L] or [Ctrl] [R] | Repeats current command line on a new line. |
| [Ctrl] [N] or ↓ | Enters the next command line in the history buffer. |
| [Ctrl] [P] or ↑ | Enters the previous command line in the history buffer. |
| [Ctrl] [U] or [Ctrl] [X] | Deletes from the cursor tothe beginning of the command line. |
| [Ctrl] [W] | Deletes the last word typed. |
| [Esc] [B] | Moves the cursor backward one word. |
| [Esc] [D] | Deletes from the cursor to the end of the word. |
| [Esc] [F] | Moves the cursor forward one word. |
| [Delete] or [Backspace] | Deletes the first character to the left of the cursor in the command line. |

# Using the Web Browser Interface

The web browser interface built into the switch lets you easily access the switch from a browser-based PC on your network. This lets you do the following:

- Optimize your network uptime by using the Alert Log and other diagnostic tools
- Make configuration changes to the switch
- Maintain security by configuring usernames and passwords

This chapter covers the following:

- General features (page 4-2).
- System requirements for using the web browser interface (page 4-3)
- Starting a web browser interface session (page 4-4)
- Tasks for your first web browser interface session (page 4-6):
  - Creating usernames and passwords in the web browser interface (page 4-7)
- Description of the web browser interface:
  - Overview window and tabs (page 4-11)
  - Port Utilization and Status displays (page 4-12)
  - Alert Log and Alert types (page 4-15)

**Note**

If you want security beyond that achieved with user names and passwords, you can disable access to the web browser interface. This is done by either executing **no web-management** at the Command Prompt or changing the **Web Agent Enabled** parameter setting to **No** (page 5-16) .

# General Features

The SMC6624M switch includes these web browser interface features:

Switch Configuration:

- Ports
- VLANs and Primary VLAN
- Port monitoring (mirroring)
- System information
- Enable/Disable Multicast Filtering (IGMP) and Spanning Tree
- IP
- Stacking
- Support URL

Switch Security:

- Passwords
- Authorized IP Managers
- Port security and Intrusion Log

Switch Diagnostics:

- Ping/Link Test
- Device reset
- Configuration report

Switch status

- Port utilization
- Port counters
- Port status
- Alert log

Switch system information listing

# Web Browser Interface Requirements

You can use equipment meeting the following requirements to access the web browser interface on your intranet.

**Table 4-1. System Requirements for Accessing the Web Browser Interface**

| Platform Entity and OS Version | Minimum | Recommended |
|---|---|---|
| PC Platform | 90 MHz Pentium | 120 MHz Pentium |
| RAM | 16 Mbytes | 32 Mbytes |
| Screen Resolution | 800 X 600 | 1,024 x 768 |
| Color Count | 256 | 65,536 |
| Internet Browser<br>(English-language browser only) | **PCs:**<br>• Netscape® Communicator 4.x<br>• Microsoft®Internet Explorer 4.x<br>**UNIX:** Netscape Navigator 4.5 or later | **PCs:**<br>• Netscape Communicator 4.5 or later<br>• Microsoft®Internet Explorer 5.0 or later<br>**UNIX:** Netscape Navigator 4.5 or later |
| PC Operating System | Microsoft Windows®95 and Windows NT | |
| UNIX®Operating System | Standard UNIX®OS | |

# Starting a Web Browser Interface Session with the Switch

You can start a web browser session in the following ways:

- Using a standalone web browser on a network connection from a PC or UNIX workstation:
  - Directly connected to your network
  - Connected through remote access to your network

## Using a Standalone Web Browser in a PC or UNIX Workstation

This procedure assumes that you have a supported web browser (page 4-3) installed on your PC or workstation, and that an IP address has been configured on the switch. (For more on assigning an IP address, refer to "IP Configuration" on page 5-2.)

1. Make sure the Java™ applets are enabled for your browser. If they are not, do one of the following:
   - In Netscape 4.03, click on **Edit, Preferences..., Advanced**, then select **Enable Java** and **Enable JavaScript** options.
   - In Microsoft Internet Explorer 4.x, click on **View**, **Internet Options**, **Security**, **Custom**, [Settings] and scroll to the **Java Permissions**. Then refer to the online Help for specific information on enabling the Java applets.
2. Type the IP address (or DNS name) of the switch in the browser **Location or Address** field and press [Enter]. (It is not necessary to include **http://**.)

   **switch6624M** [Enter](example of a DNS-type name)

   **10.11.12.195** [Enter] (example of an IP address)

   If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **switch6624M**) that you can type in the **Location or Address** field instead of the IP address. Using DNS names typically improves browser performance. See your network administrator for any name associated with the switch.

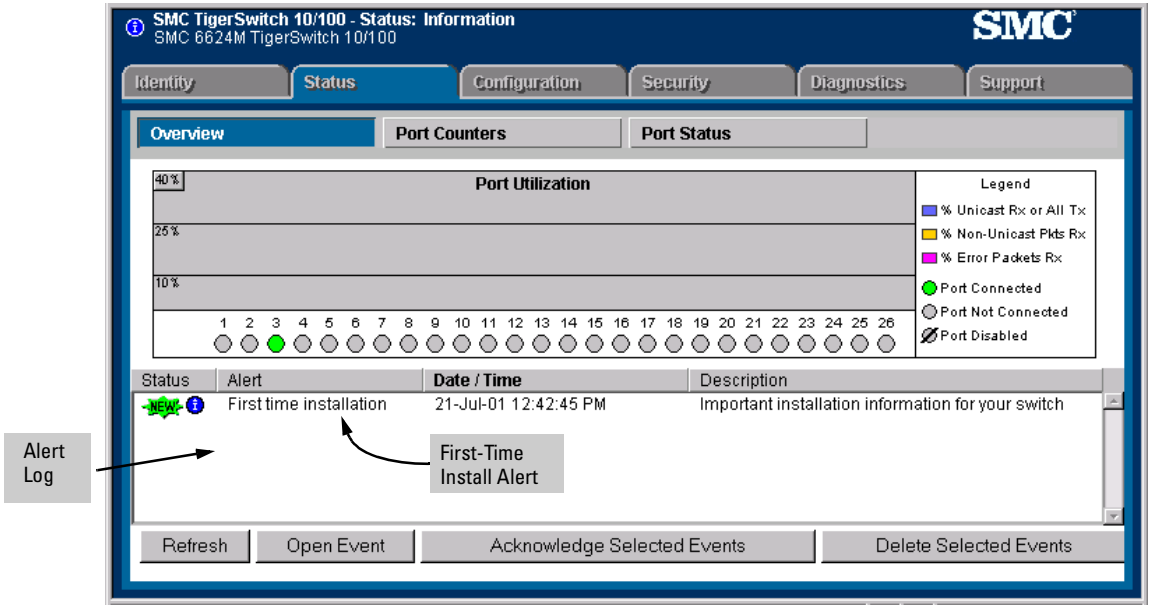



**Figure 4-1. Example of Status Overview Screen**

**Note**

The above screen appears somewhat different if the switch is configured as a stack Commander. For an example, see figure 1-3 on page 1-4.

# Tasks for Your First Web Browser Interface Session

The first time you access the web browser interface, there are three tasks that you should perform:

- Review the "First Time Install" window
- Set Manager and Operator passwords

## Viewing the "First Time Install" Window

When you access the switch's web browser interface for the first time, the Alert log contains a "First Time Install" alert, as shown in figure 4-2. This gives you information about first time installations, and provides an immediate opportunity to set passwords for security.

Double click on **First Time Install** in the Alert log (figure 4-1 on page 4-5). The web browser interface then displays the "First Time Install" window, below.

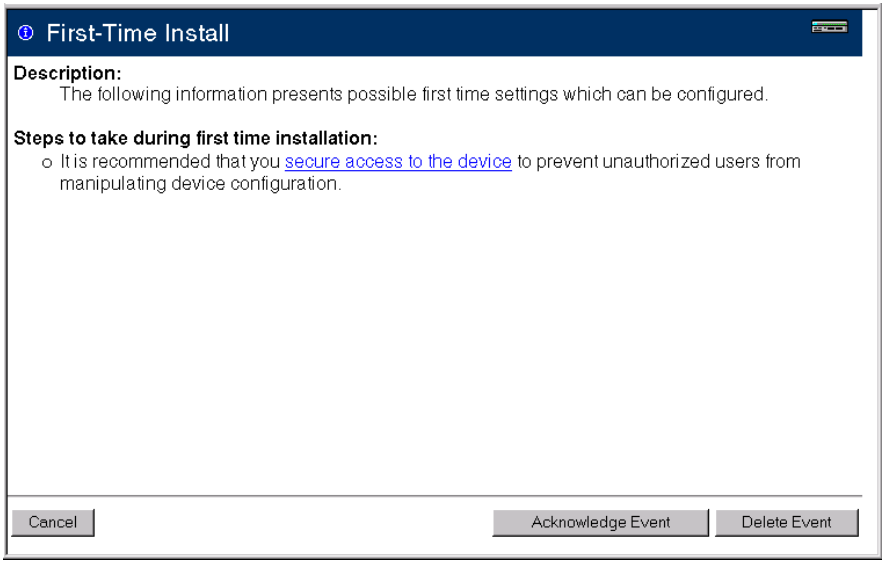



**Figure 4-2. First-Time Install Window**

This window is the launching point for the basic configuration you need to perform to set web browser interface passwords to maintain security.

To set web browser interface passwords, click on **secure access to the device** to display the Device Passwords screen, and then go to the next page. (You can also access the password screen by clicking on the **Security** tab.)

## Creating Usernames and Passwords in the Browser Interface

You may want to create both a username and password to create access security for your switch. There are two levels of access to the interface that can be controlled by setting user names and passwords:

- **Operator.** An Operator-level user name and password allows read-only access to most of the web browser interface, but prevents access to the Security window.
- **Manager.** A Manager-level user name and password allows full read/write access to the web browser interface.

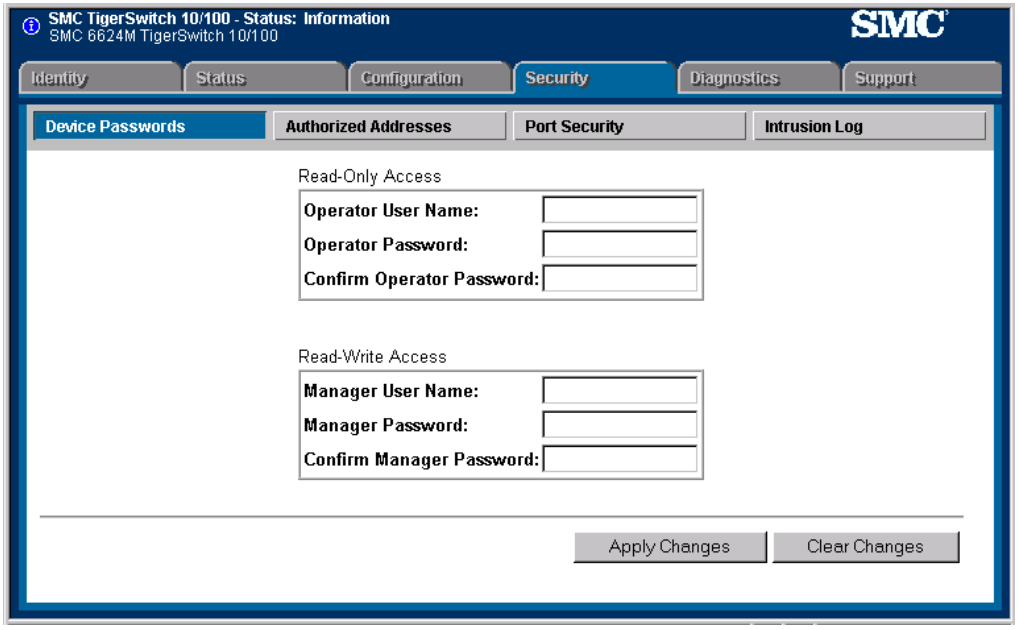



**Figure 4-3. The Device Passwords Window**

To set the passwords:

1. Access the Device Passwords screen by one of the following methods:
   - If the Alert Log includes a "First Time Install" event entry, double click on this event, then, in the resulting display, click on the **secure access to the device** link.
   - Select the **Security** tab.
2. Click in the appropriate box in the Device Passwords window and enter user names and passwords. You will be required to repeat the password strings in the confirmation boxes.

   Both the user names and passwords can be up to 16 printable ASCII characters.
3. Click on [Apply Changes] to activate the user names and passwords.

**Note**

Passwords you assign in the web browser interface will overwrite previous passwords assigned in either the web browser interface, the Command Prompt, or the switch console. That is, the most recently assigned passwords are the switch's passwords, regardless of which interface was used to assign the string.

## Using the Passwords

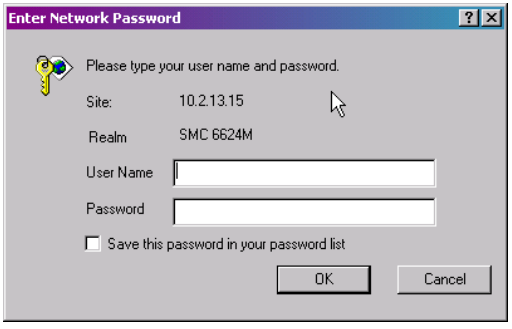



**Figure 4-4. Example of the Password Window in the Web Browser Interface**

The manager and operator passwords are used to control access to all switch interfaces. Once set, you will be prompted to supply the password every time you try to access the switch through any of its interfaces. The password you enter determines the capability you have during that session:

- Entering the manager password gives you full read/write capabilities

- Entering the operator password gives you read and limited write capabilities.

## Using the User Names

If you also set user names in the web browser interface screen, you must supply the correct user name for web browser interface access. If a user name has not been set, then leave the User Name field in the password window blank.

Note that the Command Prompt and switch console interfaces use only the password, and do not prompt you for the User Name.

## If You Lose a Password

If you lose the passwords, you can clear them by pressing the Clear button on the front of the switch. *This action deletes all password and user name protection from all of the switch's interfaces.*

*The Clear button is provided for your convenience, but its presence means that if you are concerned with the security of the switch configuration and operation, you should make sure the switch is installed in a secure location, such as a locked wiring closet.*

# Support/Mgmt URL Feature

The Support/Mgmt URL window enables you to change the World Wide Web Universal Resource Locator (URL) for a support information site for your switch.

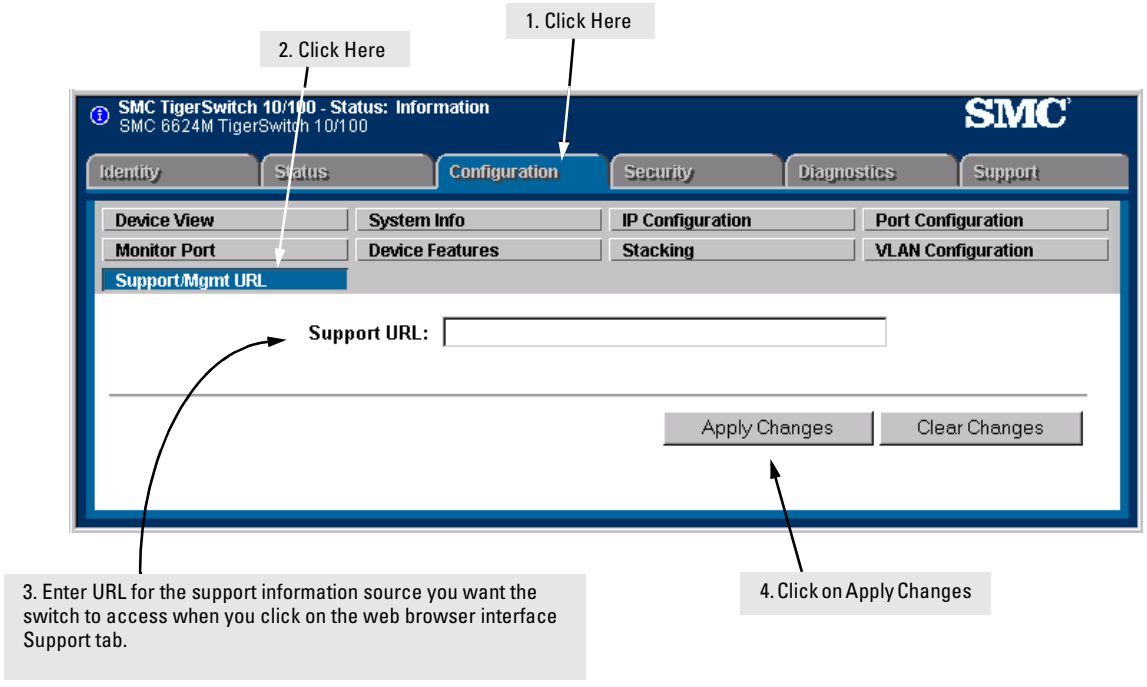



**Figure 4-5. The Default Support/Mgmt URLs Window**

## Support URL

This is the site that the switch accesses when you click on the **Support** tab on the web browser interface.

You can enter the URL for a local site that you use for entering reports about network performance, or whatever other function you would like to be able to easily access by clicking on the [Support] tab.

# Status Reporting Features

Browser elements covered in this section include:

- The Overview window (below)
- Port utilization and status (page )
- The Alert log (page )
- The Status bar (page )

## The Overview Window

The Overview Window is the home screen for any entry into the web browser interface.The following figure identifies the various parts of the screen.

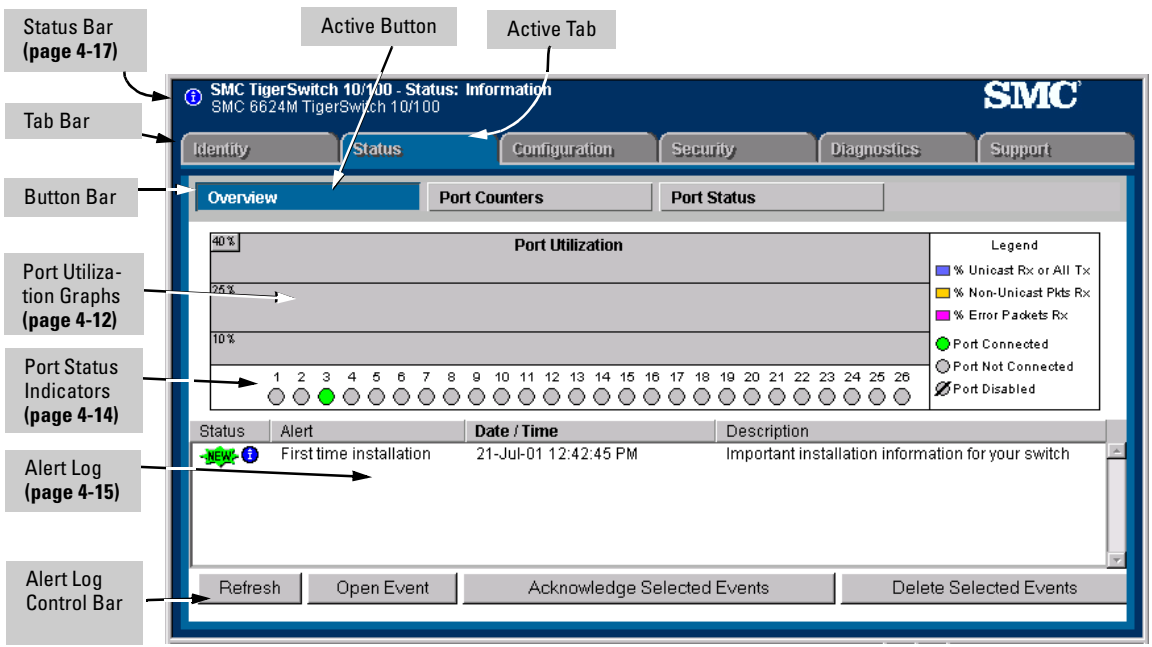



**Figure 4-6. The Overview Window**

# The Port Utilization and Status Displays

The Port Utilization and Status displays show an overview of the status of the switch and the amount of network activity on each port. The following figure shows a sample reading of the Port Utilization and Port Status.

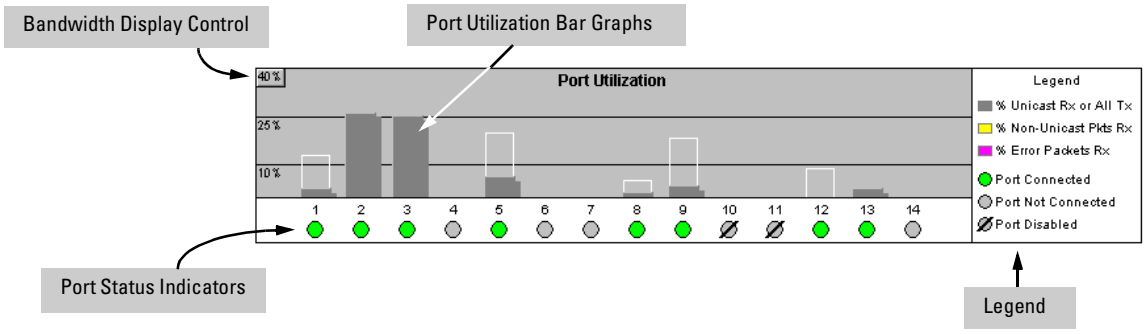



**Figure 4-7. The Graphs Area**

## Port Utilization

The Port Utilization bar graphs show the network traffic on the port with a breakdown of the packet types that have been detected (unicast packets, non-unicast packets, and error packets). The Legend identifies traffic types and their associated colors on the bar graph:

- **% Unicast Rx & All Tx:** This is all unicast traffic received and all transmitted traffic of any type. This indicator (a blue color on many systems) can signify either transmitted or received traffic.
- **% Non-Unicast Pkts Rx:** All multicast and broadcast traffic received by the port. This indicator (a gold color on many systems) enables you to know "at-a-glance" the source of any non-unicast traffic that is causing high utilization of the switch. For example, if one port is receiving heavy broadcast or multicast traffic, all ports will become highly utilized. By color-coding the received broadcast and multicast utilization, the bar graph quickly and easily identifies the offending port. This makes it faster and easier to discover the exact source of the heavy traffic because you don't have to examine port counter data from several ports.
- **% Error Pkts Rx**: All error packets received by the port. (This indicator is a reddish color on many systems.) Although errors received on a port are not propagated to the rest of the network, a consistently high number of errors on a specific port may indicate a problem on the device or network segment connected to the indicated port.

- **Maximum Activity Indicator:** As the bars in the graph area change height to reflect the level of network activity on the corresponding port, they leave an outline to identify the maximum activity level that has been observed on the port.

**Utilization Guideline.** A network utilization of 40% is considered the maximum that a typical Ethernet-type network can experience before encountering performance difficulties. If you observe utilization that is consistently higher than 40% on any port, click on the Port Counters button to get a detailed set of counters for the port.

**To change the amount of bandwidth the Port Utilization bar graph shows.** Click on the bandwidth display control button in the upper left corner of the graph. (The button shows the current scale setting, such as 40%.) In the resulting menu, select the bandwidth scale you want the graph to show (3%, 10%, 25%, 40%, 75%, or 100%), as shown in figure 3-7.

Note that when viewing activity on a gigabit port, you may want to select a lower value (such as 3% or 10%). This is because the bandwidth utilization of current network applications on gigabit links is typically minimal, and may not appear on the graph if the scale is set to show high bandwidth utilization.

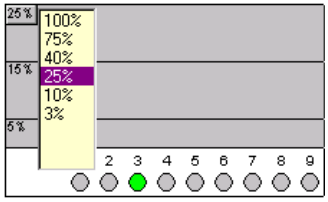



**Figure 4-8. Changing the Graph Area Scale**

**To display values for each graph bar.** Hold the mouse cursor over any of the bars in the graph, and a pop-up display is activated showing the port identification and numerical values for each of the sections of the bar, as shown in figure 4-9 (next).

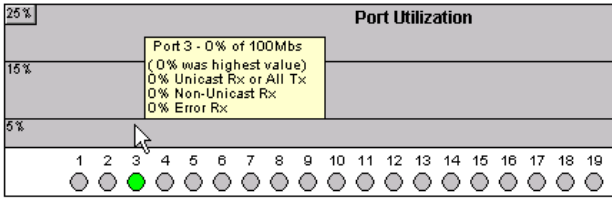



**Figure 4-9. Display of Numerical Values for the Bar**

## Port Status

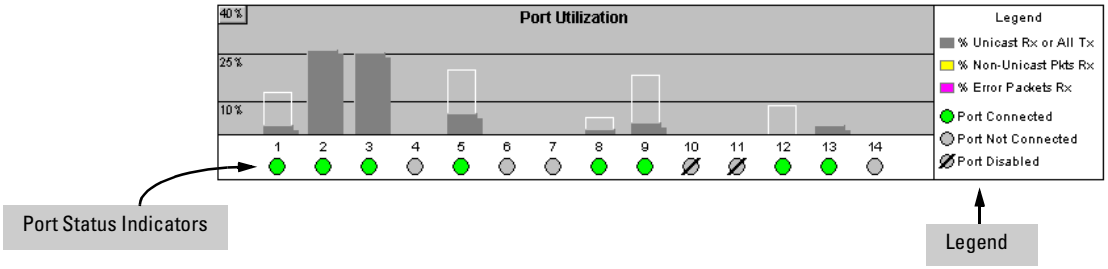



**Figure 4-10. The Port Status Indicators and Legend**

The Port Status indicators show a symbol for each port that indicates the general status of the port. There are four possible statuses:

- **Port Connected** – the port is enabled and is properly connected to an active network device.
- **Port Not Connected** – the port is enabled but is not connected to an active network device. A cable may not be connected to the port, or the device at the other end may be powered off or inoperable, or the cable or connected device could be faulty.
- **Port Disabled** – the port has been configured as disabled through the web browser interface, the switch console, or SNMP network management.
- **Port Fault-Disabled** – a fault condition has occurred on the port that has caused it to be auto-disabled. Note that the Port Fault-Disabled symbol will be displayed in the legend only if one or more of the ports is in that status. See chapter 7, “Monitoring and Analyzing Switch Operation” for more information.

# The Alert Log

The web browser interface Alert Log, shown in the lower half of the screen, shows a list of network occurrences, or *alerts*, that were detected by the switch. Typical alerts are **Broadcast Storm**, indicating an excessive number of broadcasts received on a port, and **Problem Cable**, indicating a faulty cable. A full list of alerts is shown in the table on page 4-16.

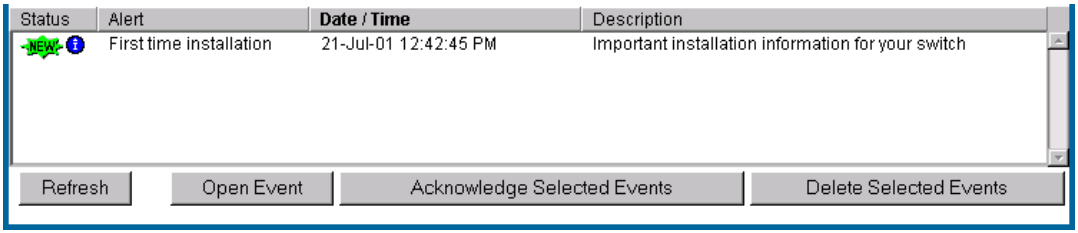



**Figure 4-11. Example of the Alert Log**

Each alert has the following fields of information:

- **Status** – The level of severity of the event generated. Severity levels can be Information, Normal, Warning, and Critical. If the alert is new (has not yet been acknowledged), the New symbol is also in the Status column.
- **Alert** – The specific event identification.
- **Date/Time** – The date and time the event was received by the web browser interface. This value is shown in the format: ***DD-MM-YY HH:MM:SS*** **AM/PM**, for example, **16-Sep-99 7:58:44 AM**.
- **Description** – A short narrative statement that describes the event. For example, **Excessive CRC/Alignment errors on port: 8**.

## Sorting the Alert Log Entries

The alerts are sorted, by default, by the Date/Time field with the most recent alert listed at the top of the list. The second most recent alert is displayed below the top alert and so on. If alerts occurred at the same time, the simultaneous alerts are sorted by order in which they appear in the MIB.

The alert field that is being used to sort the alert log is indicated by which column heading is in bold. You can sort by any of the other columns by clicking on the column heading. The Alert and Description columns are sorted alphabetically, while the Status column is sorted by severity type, with more critical severity indicators appearing above less critical indicators.

## Alert Types

The following table lists the types of alerts that can be generated.

**Table 4-2. Alert Strings and Descriptions**

| Alert String | Alert Description |
|---|---|
| First Time Install | Important installation information for your switch. |
| Too many undersized/ giant packets | A device connected to this port is transmitting packets shorter than 64 bytes or longer than 1518 bytes (longer than 1522 bytes if tagged), with valid CRCs (unlike runts, which have invalid CRCs). |
| Excessive jabbering | A device connected to this port is incessantly transmitting packets ("jabbering"), detected as oversized packets with CRC errors. |
| Excessive CRC/alignment errors | A high percentage of data errors has been detected on this port. Possible causes include:<br>• Faulty cabling or invalid topology.<br>• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)<br>• A malfunctioning NIC, NIC driver, or transceiver |
| Excessive late collisions | Late collisions (collisions detected after transmitting 64 bytes) have been detected on this port. Possible causes include:<br>• An overextended LAN topology<br>• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)<br>• A misconfigured or faulty device connected to the port |
| High collision or drop rate | A large number of collisions or packet drops have occurred on the port. Possible causes include:<br>• A extremely high level of traffic on the port<br>• Duplex mismatch<br>• A misconfigured or malfunctioning NIC or transceiver on a device connected to this port<br>• A topology loop in the network |
| Excessive broadcasts | An extremely high percentage of broadcasts was received on this port. This degrades the performance of all devices connected to the port. Possible causes include:<br>• A network topology loop—this is the usual cause<br>• A malfunctioning device, NIC, NIC driver, or software package |
| Network Loop | Network loop has been detected by the switch. |
| Loss of Link | Lost connection to one or multiple devices on the port. |
| Loss of stack member | The  Commander has lost the connection to a stack member. |
| Security violation | A security violation has occurred. |

**Note**

When troubleshooting the sources of alerts, it may be helpful to check the switch's Port Status and Port Counter windows and the Event Log in the console interface.

### Viewing Detail Views of Alert Log Entries

By double clicking on Alert Entries, the web browser interface displays a Detail View or separate window detailing information about the events. The Detail View contains a description of the problem and a possible solution. It also provides four management buttons:

- **Acknowledge Event** – removes the New symbol from the log entry
- **Delete Event** – removes the alert from the Alert Log
- **Cancel Button** – closes the detail view with no change to the status of the alert and returns you to the Overview screen.

## The Status Bar

The Status Bar is displayed in the upper left corner of the web browser interface screen. Figure 4-12 shows an expanded view of the status bar.

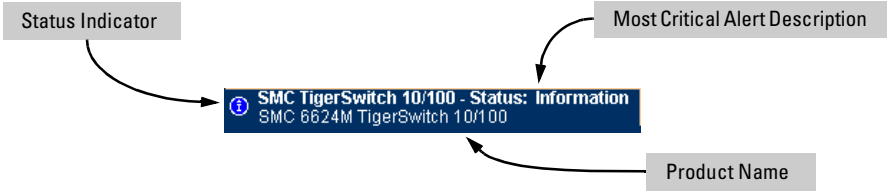



**Figure 4-12. Example of the Status Bar**

The Status bar consists of four objects:

- **Status Indicator.** Indicates, by icon, the severity of the most critical alert in the current display of the Alert Log. This indicator can be one of three shapes and colors as shown in the following table.

**Table 4-3. Status Indicator Key**

| Color | Switch Status | Status Indicator Shape |
|---|---|---|
| Blue | Normal Activity; "First time installation" information available in the Alert log. | |
| Green | Normal Activity | |
| Yellow | Warning | |
| Red | Critical | |

- **System Name.** The name you have configured for the switch by using Identity screen, **system name** command, or the switch console **System Information** screen.
- **Most Critical Alert Description.** A brief description of the earliest, unacknowledged alert with the current highest severity in the Alert Log, appearing in the right portion of the Status Bar. In instances where multiple critical alerts have the same severity level, only the earliest unacknowledged alert is deployed in the Status bar.
- **Product Name.** The product name of the switch to which you are connected in the current web browser interface session.

# Configuring IP Addressing, Interface Access, and System Information



This chapter describes the switch configuration features available in the menu interface, CLI and web browser interface. For help on how to use these interfaces, refer to:

- Chapter 2, "Using the Menu Interface"
- Chapter 3, "Using the Command Line Interface (CLI)"
- Chapter 4, Using the Web Browser Interface"

**Why Configure IP Addressing?** In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by the ports on the switch. However, to enable specific management access and control through your network, you will need IP addressing. (See table 5-1 on page 5-10.)

**Why Configure Interface Access and System Information?** The interface access features in the switch operate properly by default. However, you can modify or disable access features to suit your particular needs. Similarly, you can choose to leave the system information parameters at their default settings. However, using these features can help you to more easily manage a group of devices across your network.

# IP Configuration

### IP Configuration Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| IP Address and Subnet Mask | DHCP/Bootp | page 5-4 | page 5-6 | page 5-9 |
| Default Gateway Address | none | page 5-4 | page 5-6 | page 5-9 |
| Packet Time-To-Live (TTL) | 64 seconds | page 5-4 | page 5-6 | n/a |
| Time Server (Timep) | DHCP | page 5-4 | page 5-6 | n/a |

**IP Address and Subnet Mask.** Configuring the switch with an IP address expands your ability to manage the switch and use its features. By default, the switch is configured to automatically receive IP addressing on the default VLAN from a DHCP/Bootp server that has been configured correctly with information to support the switch. (Refer to "DHCP/Bootp Operation" on page 5-10 for information on setting up automatic configuration from a server.) However, if you are not using a DHCP/Bootp server to configure IP addressing, use the menu interface or the CLI to manually configure the initial IP values. After you have network access to a device, you can use the web browser interface to modify the initial IP configuration if needed.

For information on how IP addressing affects switch performance, refer to "How IP Addressing Affects Switch Operation" on page 5-9.

**Default Gateway Operation.** The default gateway is required when a router is needed for tasks such as reaching off-subnet destinations or forwarding traffic across multiple VLANs. The gateway value is the IP address of the next-hop gateway node for the switch, which is used if the requested destination address is not on a local subnet/VLAN. If the switch does not have a manually-configured default gateway and DHCP/Bootp is configured on the primary VLAN, then the default gateway value provided by the DHCP or Bootp server will be used. If the switch has a manually configured default gateway, then the switch uses this gateway, even if a different gateway is received via DHCP or Bootp on the primary VLAN. See "Notes" on page 5-3 and "Which VLAN Is Primary?" on page 9-51.

**Packet Time-To-Live (TTL).** This parameter specifies how long in seconds an outgoing packet should exist in the network. In most cases, the default setting (64 seconds) is adequate.

**Timep Operation.** Use this optional parameter if you want the switch to get its time information from another device operating as a Timep server. In its default Timep configuration, the switch attempts to get a Timep server address from a DHCP server. Other configuration options are to manually assign a Timep server address or to disable the Timep server feature.

## Just Want a Quick Start?

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, SMC recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

- Enter setup at the CLI Manager level prompt.

```
SMC TigerSwitch 10/100# setup
```

- Select **8. Run Setup** in the Main Menu of the menu interface.

For more on using the Switch Setup screen, see the *Installation Guide* you received with the switch.

## IP Addressing with Multiple VLANs

In the factory-default configuration, the switch has one, permanent default VLAN (named DEFAULT_VLAN) that includes all ports on the switch. In this state, when you assign an IP address and subnet mask to the switch, you are actually assigning the IP addressing to the DEFAULT_VLAN. You can rename the DEFAULT_VLAN, but you cannot change its VLAN ID number (VID) or remove it from the switch.

**Notes**

- If multiple VLANs are configured, then each VLAN can have its own IP address. This is because each VLAN operates as a separate broadcast domain and requires a unique IP address and subnet mask. A default gateway (IP) address for the switch is optional, but recommended. The *primary* VLAN is the VLAN used for stacking operation, as well as for determining the default gateway address, (packet) Time-To-Live (TTL), and Timep via DHCP or Bootp. (Other VLANs can also use DHCP or BootP to acquire IP addressing. However, the switch's gateway, TTL, and TimeP values will be acquired through the primary VLAN only. In the default configuration, the default VLAN (named DEFAULT_VLAN) is the switch's primary VLAN.However, with multiple VLANs assigned to the switch, you can select another VLAN to function as the primary VLAN. For more on VLANs, refer to "Port-Based Virtual LANs (Static VLANs)" on page 9-48.

- The IP addressing used in the switch should be compatible with your network. That is, the IP address must be unique and the subnet mask must be appropriate for the IP network.
- If you plan to connect to other networks that use globally administered IP addresses, refer to "Globally Assigned IP Network Addresses" on page 5-14.
- By default, the switch uses DHCP to acquire the IP address of the TimeP server. If the switch does not have a manually configured Timep setting, then it attempts to get its TimeP setting through DHCP or Bootp through the primary VLAN.
- The switch searches for the default gateway device through the primary VLAN. By default, the DEFAULT_VLAN is the switch's primary VLAN. However, you can use the CLI to select a different primary VLAN if more than one VLAN exists on the switch. For more information, see "Port-Based Virtual LANs (Static VLANs)" on page 9-48.
- If you change the IP address through either Telnet access or the web browser interface, the connection to the switch will be lost. You can reconnect by either restarting Telnet with the new IP address or entering the new address as the URL in your web browser.

## IP Addressing in a Stacking Environment

If you are installing the switch into a stack management environment, entering an IP address may not be required. See "Stack Management" on page 9-2 for more information.

## Menu: Configuring IP Address, Gateway, Time-To-Live (TTL), and Timep

Do one of the following:

- To manually enter an IP address, subnet mask, set the **IP Config** parameter to **Manual** and then manually enter the IP address and subnet mask values you want for the switch.
- To use DHCP or Bootp, use the menu interface to ensure that the **IP Config** parameter is set to **DHCP/Bootp**, then refer to "DHCP/Bootp Operation" on page 5-10.

**To Configure IP Addressing.**

1. From the Main Menu, Select.
   **2. Switch Configuration ...**
   **5. IP Configuration**

**Note**

If multiple VLANs are configured, a screen showing all VLANs appears instead of the following screen.

The default setting for **TimeP Config** is DHCP. Setting it to **Manual**, then pressing ↓ or [Tab] causes the **Server Address** parameter to appear.

For descriptions of these parameters, see the online Help for this screen.

Before using the DHCP/ Bootp option, refer to "DHCP/Bootp Operation" on page 5-10.

```
============================- CONSOLE - MANAGER MODE -=============================
                  Switch Configuration - Internet (IP) Service


  Default Gateway :
  Default TTL     : 64

  TimeP Config [DHCP] : DHCP
  TimeP Poll Interval (min) [720] : 720

  IP Config [DHCP/Bootp] : DHCP/Bootp
  IP Address  :
  Subnet Mask :

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 5-1. Example of the IP Service Configuration Screen without Multiple VLANs Configured**

2. Press [E] (for **Edit**).
3. If the switch needs to access a router, for example, to reach off-subnet destinations, select the **Default Gateway** field and enter the IP address of the gateway router.
4. If you need to change the packet Time-To-Live (TTL) setting, select **Default TTL** and type in a value between 2 and 255 (seconds).
5. At the **TimeP Config** field do one of the following:
   - If you want the switch to obtain the IP address of the Timep server via DHCP server, keep the value as **DHCP**.
   - If you want to manually specify the IP address of the Timep server, use the Space bar to select **Manual**.
   - If you don't have a Timep server set up, use the Space bar to change the value to **Disabled**.

6. If you selected **Manual** , press [Tab] or [↓], and additional fields will be displayed for entering the IP address for the Timep server.
7. Select the **TimeP Poll Interval** field if you want to change the value for how often the switch polls the Timep server for time information.
8. Do one of the following:
   - If you want to have the switch retrieve its IP configuration from a DHCP or Bootp server, at the **IP Config** field, keep the value as **DHCP/ Bootp** and go to step 11.
   - If you want to manually configure the IP information, use the Space bar to select **Manual** and use the [Tab] key to move to the other IP configuration fields.
9. Select the **IP Address** field and enter the IP address for the switch.
10. Select the **Subnet Mask** field and enter the subnet mask for the IP address.
11. Press [Enter], then [S] (for **Save**).

## CLI: Configuring IP Address, Gateway, Time-To-Live (TTL), and Timep

**IP Commands Used in This Section**

| | |
|---|---|
| show ip | page 5-7 |
| vlan *<vlan-id>* ip address | page 5-8 |
| ip default-gateway | page 5-8 |
| ip ttl | page 5-8 |
| [no] ip timep | page 5-9 |

**Viewing the Current IP Configuration.** The following command displays the IP addressing for each VLAN configured in the switch. If only the DEFAULT_VLAN exists, then its IP configuration applies to all ports in the switch. Where multiple VLANs are configured, the IP addressing is listed per VLAN. The display includes switch-wide packet time-to-live, and (if configured) the switch's default gateway and Timep configuration.

***Syntax:*** show ip

For example, in the factory-default configuration (no IP addressing assigned), the switch's IP addressing appears as:

The Default IP Configuration on the SMC6624M

```
SMC TigerSwitch 10/100# show ip

 Internet (IP) Service


  Default Gateway :
  Default TTL     : 64

  VLAN         | IP Config  IP Address      Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | DHCP/Bootp
```

**Figure 5-2. Example of the Switch's Default IP Addressing**

With multiple VLANs and some other features configured, **show ip** provides additional information:

An SMC6624M with VLANs Configured

```
SMC TigerSwitch 10/100# show ip

 Internet (IP) Service


  Default Gateway : 10.2.64.254
  Default TTL     : 64

  VLAN         | IP Config  IP Address      Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | Manual     10.2.13.15      255.255.0.0
  VLAN_2       | DHCP/Bootp
```

**Figure 5-3. Example of Show IP Listing with Non-Default IP Addressing Configured**

(If DHCP/Bootp acquires an IP address and Subnet Mask for VLAN_2, they will appear in the appropriate columns.)

**Configure an IP Address and Subnet Mask.** The following command includes both the IP address and the subnet mask. You must either include the ID of the VLAN for which you are configuring IP addressing or go to the context configuration level for that VLAN. (If you are not using VLANs on the switch—that is, if the only VLAN is the default VLAN—then the VLAN ID is always "1".)

**Note**

The default IP address setting for the DEFAULT_VLAN is **DHCP/Bootp**. On additional VLANs you create, the default IP address setting is **Disabled**.

***Syntax:*** vlan *<vlan-id>* ip address *<ip-address/mask-length>*
or
vlan *<vlan-id>* ip address *<ip-address> <mask-bits>*
or
vlan *<vlan-id>* ip address *dhcp-bootp*

This example configures IP addressing on the default VLAN with the subnet mask specified in mask bits.

```
SMC TigerSwitch 10/100(config)# vlan 1 ip address 10.28.227.103/
255.255.255.0
```

This example configures the same IP addressing as the preceding example, but specifies the subnet mask by mask length.

```
SMC TigerSwitch 10/100(config)# vlan 1 ip address 10.28.227.103/
24
```

**Configure the Optional Default Gateway.** You can assign one default gateway to the switch.

***Syntax:*** ip default-gateway *<ip-address>*

For example:

```
SMC TigerSwitch 10/100(config)# ip default-gateway
11.28.227.115
```

You can execute this command only from the global configuration level.

**Configure Time-To-Live (TTL).** This command sets the time that a packet outbound from the switch can exist on the network. The default setting is 64 seconds.

***Syntax:*** ip ttl *<number-of-seconds>*

```
SMC TigerSwitch 10/100(config)# ip ttl 60
```

In the CLI, you can execute this command only from the global configuration level. The TTL range is 2 - 255 seconds.

**Configure the Optional Timep Server.**

***Syntax:*** [no] ip timep <dhcp | manual *<ip-address>* > [interval <1-9999>]

You can specify whether the address of the Timep server is assigned via DHCP or manually, and the interval in minutes between Timep queries (1-9999 minutes; default 720 minutes). The following examples show the Timep command options:

```
SMC TigerSwitch 10/100(config)# ip timep manual 10.28.227.1
interval 60

SMC TigerSwitch 10/100(config)# ip timep manual 10.28.227.1

SMC TigerSwitch 10/100(config)# ip timep dhcp

SMC TigerSwitch 10/100(config)# ip timep dhcp interval 60

SMC TigerSwitch 10/100(config)# no ip timep
```

## Web: Configuring IP Addressing

You can use the web browser interface to access IP addressing only if the switch already has an IP address that is reachable through your network.

1. Click on the Configuration tab.
2. Click on [IP Configuration].

## How IP Addressing Affects Switch Operation

Without an IP address and subnet mask compatible with your network, the switch can be managed only through a direct terminal device connection to the Console RS-232 port. You can use direct-connect console access to take advantage of features that do not depend on IP addressing. However, to realize the full performance capabilities proactive networking offers through the switch, configure the switch with an IP address and subnet mask compatible with your network. The following table lists the general features available with and without a network-compatible IP address configured.

**Table 5-1. Features Available With and Without IP Addressing on the Switch**

| Features Available Without an IP Address | Additional Proactive Networking Features Available with an IP Address and Subnet Mask |
|---|---|
| • Direct-connect access to the CLI and the menu interface.<br>• Stacking Candidate or Stack Member<br>• DHCP or Bootp support for automatic IP address configuration, and DHCP support for automatic Timep server IP address configuration<br>• Spanning Tree Protocol<br>• Port settings and port trunking<br>• Console-based status and counters information for monitoring switch operation and diagnosing problems through the CLI or menu interface.<br>• VLANs<br>• GVRP<br>• Serial downloads of operating system (OS) updates and configuration files (Xmodem)<br>• Link test<br>• Port monitoring<br>• Security | • Web browser interface access, with configuration, security, and diagnostic tools, plus the Alert Log for discovering problems detected in the switch along with suggested solutions<br>• SNMP network management access such as EliteView network configuration, monitoring, problem-finding and reporting, analysis, and recommendations for changes to increase control and uptime<br>• Stacking Commander*<br>• Telnet access to the CLI or the menu interface<br>• IGMP<br>• Timep server configuration<br>• TFTP download of configurations and OS updates<br>• Ping test |

*Although a Commander can operate without an IP address, doing so makes it unavailable for in-band access in an IP network.

## DHCP/Bootp Operation

**Overview.** DHCP/Bootp is used to provide configuration data from a DHCP or Bootp server to the switch. This data can be the IP address, subnet mask, default gateway, Timep Server address, and TFTP server address. If a TFTP server address is provided, this allows the switch to TFTP a previously saved configuratin file from the TFTP server to the switch. With either DHCP or Bootp, the servers must be configured prior to the switch being connected to the network.

**Note**

The SMC6624M switch is compatible with both DHCP and Bootp servers.

**The DHCP/Bootp Process.** Whenever the **IP Config** parameter in the switch or in an individual VLAN in the switch is configured to **DHCP/Bootp** (the default), or when the switch is rebooted with this configuration:

1. DHCP/Bootp requests are automatically broadcast on the local network. (The switch sends one type of request to which either a DHCP or Bootp server can respond.)
2. When a DHCP or Bootp server receives the request, it replies with a previously configured IP address and subnet mask for the switch. The switch also receives an IP Gateway address if the server has been configured to provide one. In the case of Bootp, the server must first be configured with an entry that has the MAC address of the switch. (To determine the switch's MAC address, see appendix B, "MAC Address Management". The switch properly handles replies from either type of server. If multiple replies are returned, the switch tries to use the first reply.)

**Note**

If you manually configure a gateway on the switch, it will ignore any gateway address received via DHCP or Bootp.

If the switch is initially configured for DHCP/Bootp operation (the default), or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process immediately.

**DHCP Operation.** A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic. Depending on how the DHCP server is configured, the switch may receive an IP address that is temporarily leased. Periodically the switch may be required to renew its lease of the IP configuration. Thus, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. However, you can fix the address assignment for the switch by doing either of the following:

- Configure the server to issue an "infinite" lease.
- Using the switch's MAC address as an identifier, configure the server with a "Reservation" so that it will always assign the same IP address to the switch. (For MAC address information, refer to appendix B, "MAC Address Management".)

For more information on either of these procedures, refer to the documentation provided with the DHCP server.

**Bootp Operation.** When a Bootp server receives a request it searches its Bootp database for a record entry that matches the MAC address in the Bootp request from the switch. If a match is found, the configuration data in the associated database record is returned to the switch. For many Unix systems, the Bootp database is contained in the **/etc/bootptab** file. In contrast to DHCP operation, Bootp configurations are always the same for a specific receiving device. That is, the Bootp server replies to a request with a configuration previously stored in the server and designated for the requesting device.

**Bootp Database Record Entries.** A minimal entry in the Bootp table file **/etc/bootptab** to update an IP address and subnet mask to the switch or a VLAN configured in the switch would be similar to this entry:

```
6624mswitch:\
   ht=ether:\
   ha=0030c1123456:\
   ip=10.66.77.88:\
   sm=255.255.248.0:\
   gw=10.66.77.1:\
   hn:\
   vm=rfc1048
```

An entry in the Bootp table file `/etc/bootptab` to tell the switch or VLAN where to obtain a configuration file download would be similar to this entry:

```
6624mswitch:\
   ht=ether:\
   ha=0030c1123456:\
   ip=10.66.77.88:\
   sm=255.255.248.0:\
   gw=10.66.77.1:\
   lg=10.22.33.44:\
   T144="switch.cfg":\
   vm=rfc1048
```

*where:*

| | |
|---|---|
| 6624mswitch | is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you should use a unique symbolic name for each switch. |
| ht | is the "hardware type". For the SMC6624M, set this to **ether** (for Ethernet). *This tag must precede the* ha *tag.* |
| ha | is the "hardware address". Use the switch's (or VLAN's) 12-digit MAC address. |
| ip | is the IP address to be assigned to the switch (or VLAN). |
| sm | is the subnet mask of the subnet in which the switch (or VLAN) is installed. |

| | |
|---|---|
| gw | is the IP address of the default gateway. |
| lg | TFTP server address (source of final configuration file) |
| T144 | is the vendor-specific "tag" identifying the configuration file to download. |
| vm | is a required entry that specifies the Bootp report format. For the SMC6624M, set this parameter to **rfc1048**. |

**Note**

The above Bootp table entry is a sample that will work for the SMC6624M when the appropriate addresses and file names are used.



## Network Preparations for Configuring DHCP/Bootp

In its default configuration, the switch is configured for DHCP/Bootp operation. However, the DHCP/Bootp feature will not acquire IP addressing for the switch unless the following tasks have already been completed:

- For Bootp operation:
  - A Bootp database record has already been entered into an appropriate Bootp server.
  - The necessary network connections are in place
  - The Bootp server is accessible from the switch
- For DHCP operation:
  - A DHCP scope has been configured on the appropriate DHCP server.
  - The necessary network connections are in place
  - A DHCP server is accessible from the switch

**Note**

Designating a primary VLAN other than the default VLAN affects the switch's use of information received via DHCP/Bootp. For more on this topic, see "Which VLAN Is Primary?" on page 9-51.

After you reconfigure or reboot the switch with DHCP/Bootp enabled in a network providing DHCP/Bootp service, the switch does the following:

- Receives an IP address and subnet mask and, if configured in the server, a gateway IP address and the address of a Timep server.
- If the DHCP/Bootp reply provides information for downloading a configuration file, the switch uses TFTP to download the file from the designated source, then reboots itself. (This assumes that the switch or VLAN has connectivity to the TFTP file server specified in the reply, that the configuration file is correctly named, and that the configuration file exists in the TFTP directory.)

## Globally Assigned IP Network Addresses

If you intend to connect your network to other networks that use globally administered IP addresses, SMC strongly recommends that you use IP addresses that have a network address assigned to you. There is a formal process for assigning unique IP addresses to networks worldwide. For more information:

Please contact your internet service provider (ISP).

If you need more information than your ISP can provide, contact one of the following organizations:

| Country | Phone Number/E-Mail/URL | Company Name/Address |
|---|---|---|
| United States/ Countries not in Europe or Asia/Pacific | 1-310-823-9358<br>icann@icann.org<br>http://www.iana.org | The Internet Corporation for Assigned Names and Numbers (ICANN)<br>4676 Admiralty Way, Suite 330<br>Marina Del Rey, CA 90292<br>USA |
| Europe | +31 20 535 4444<br>ncc@ripe.net<br>http://www.ripe.net | RIPE NCC<br>Singel 258<br>1016 AB Amsterdam<br>The Netherlands |
| Asia/Pacific | +61-7-3367-0490<br>info@apnic.net<br>http://www.apnic.net | Attention: IN-ADDR.ARPA Registration<br>Asia Pacific Network Information Center<br>Level 1, 33 Park Road<br>PO Box 2131<br>Milton, QLD 4064<br>Australia |

For more information, refer to *Internetworking with TCP/IP: Principles, Protocols and Architecture* by Douglas E. Comer (Prentice-Hall, Inc., publisher).

# Interface Access: Console/Serial Link, Web, and Inbound Telnet



### Interface Access Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Inactivity Time | 0 Minutes (disabled) | page 5-16 | page 5-18 | — |
| Inbound Telnet Access | Enabled | page 5-16 | page 5-17 | — |
| Web Browser Interface Access | Enabled | page 5-16 | page 5-18 | — |
| Terminal type | VT-100 | — | page 5-18 | — |
| Event Log event types to list (Displayed Events) | All | — | page 5-18 | — |
| Baud Rate | Speed Sense | — | page 5-18 | — |
| Flow Control | XON/XOFF | — | page 5-18 | — |

In most cases, the default configuration is acceptable for standard operation.

**Note**

Basic switch security is through passwords. You can gain additional security using IP authorized managers. However if unauthorized access to the switch through in-band means (Telnet or the web browser interface), then you can disallow in-band access (as described in this section) and install the switch in a locked environment.

## Menu: Modifying the Interface Access

The menu interface enables you to modify these parameters:

- Inactivity Timeout
- Inbound Telnet Enabled
- Web Agent Enabled

**To Access the Interface Access Parameters:**

1. From the Main Menu, Select...
   **2. Switch Configuration...**
   **1. System Information**

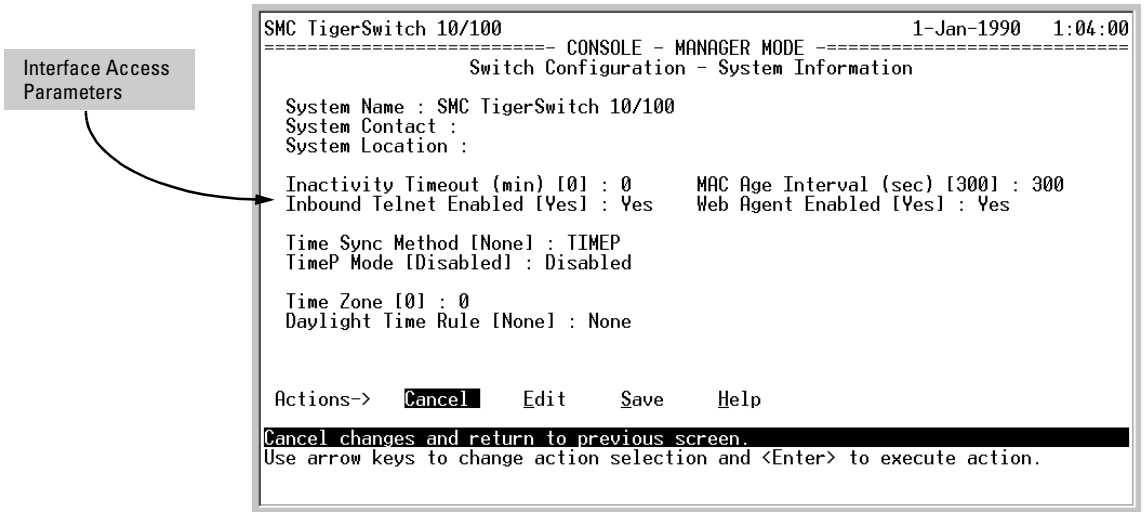



**Figure 5-4. The Default Interface Access Parameters Available in the Menu Interface**

2. Press [E] (for Edit). The cursor moves to the **System Name** field.
3. Use the arrow keys ([↓], [↑], [←], [→]) to move to the parameters you want to change.

   Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press [Enter], then press [S] (for **Save**).

# CLI: Modifying the Interface Access

### Interface Access Commands Used in This Section

| | |
|---|---|
| show console | below |
| [no] telnet-server | below |
| [no] web-management | page 5-18 |
| console | page 5-18 |

**Listing the Current Console/Serial Link Configuration.** This command lists the current interface access parameter settings.

***Syntax***: show console

This example shows the switch's default console/serial configuration.

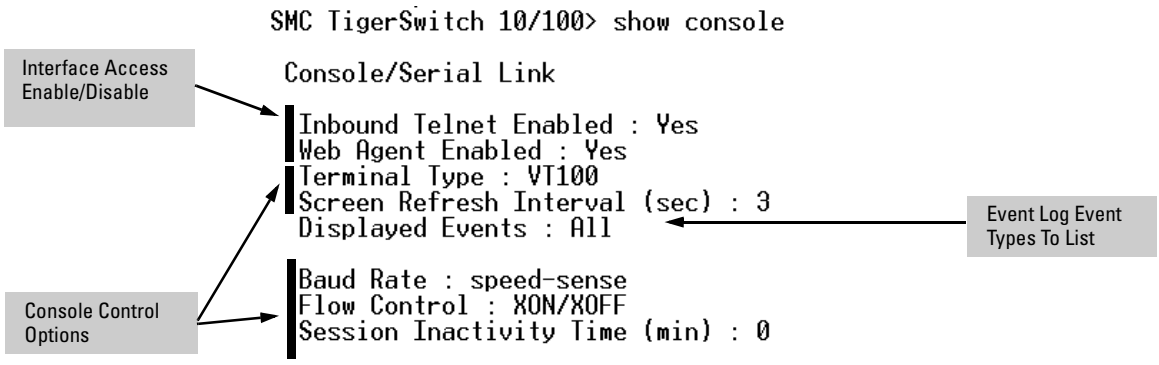



**Figure 5-5. Listing of Show Console Command**

**Reconfigure Inbound Telnet Access.** In the default configuration, inbound Telnet access is enabled.

***Syntax:***[no] telnet-server

To disable inbound Telnet access:

```
SMC TigerSwitch 10/100(config)# no telnet-server
```

To re-enable inbound Telnet access:

```
SMC TigerSwitch 10/100(config)# telnet-server
```

**Reconfigure Web Browser Access.** In the default configuration, web browser access is enabled.

***Syntax:***[no] web-management

To disable web browser access:

```
SMC TigerSwitch 10/100(config)# no web-management
```

To re-enable web browser access:

```
SMC TigerSwitch 10/100(config)# web-management
```

**Reconfigure the Console/Serial Link Settings.** You can reconfigure one or more console parameters with one console command.

***Syntax:*** console
[terminal <vt100 | ansi>]
[screen-refresh <1 | 3 | 5 | 10 | 20 | 30 | 45 | 60>]
[baud <speed-sense | 1200 | 2400 | 4800 | 9600 | 19200 |38400 | 57600>]
[flow-control <xon/xoff | none>]
[inactivity-timer <0 1 5 10 15 20 30 60 120>]
[events <none | all | non-info | critical | debug]

**Note**

If you change the Baud Rate or Flow Control settings for the switch, you should make the corresponding changes in your console access device. Otherwise, you may lose connectivity between the switch and your terminal emulator due to differences between the terminal and switch settings for these two parameters.

All console parameter changes except **events** require that you save the configuration with **write memory** and then execute **boot** before the new console configuration will take effect.

For example, to use one command to configure the switch with the following:

- VT100 operation
- 19,200 baud
- No flow control
- 10-minute inactivity time
- Critical log events

you would use the following command sequence:

```
SMC TigerSwitch 10/100(config)# console terminal vt100 baud 19200 flow-control n
one inactivity-timer 10 events critical
Command will take effect after saving configuration and reboot.
SMC TigerSwitch 10/100(config)# write memory
SMC TigerSwitch 10/100(config)# reload
```

The switch implements the Event Log change immediately. The switch implements the other console changes after executing **write memory** and **reload**.

**Figure 5-6. Example of Executing the Console Command with Multiple Parameters**

You can also execute a series of console commands and then save the configuration and boot the switch. For example:

Configure the individual parameters.

Save the changes.

Boot the switch.

```
SMC TigerSwitch 10/100(config)# console baud speed-sense
Command will take effect after saving configuration and reboot.
SMC TigerSwitch 10/100(config)# console flow-control xon/xoff
Command will take effect after saving configuration and reboot.
SMC TigerSwitch 10/100(config)# console inactivity-timer 0
Command will take effect after saving configuration and reboot.
SMC TigerSwitch 10/100(config)# write memory
SMC TigerSwitch 10/100(config)# reload
```

**Figure 5-7. Example of Executing a Series of Console Commands**

# System Information

### System Information Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| System Name | *switch product name* | page 5-21 | page 5-22 | page 5-24 |
| System Contact | n/a | page 5-21 | page 5-22 | page 5-24 |
| System Location | n/a | page 5-21 | page 5-22 | page 5-24 |
| MAC Age Interval | 300 seconds | page 5-21 | page 5-23 | — |
| Time Zone | 0 | page 5-21 | page 5-23 | — |
| Daylight Time Rule | None | page 5-21 | page 5-23 | — |
| Time | January 1, 1990 at 00:00:00 at last power reset | — | page 5-24 | — |

Configuring system information is optional, but recommended.

**System Name:** Using a unique name helps you to identify individual devices in stacking environments and where you are using an SNMP network management tool such as EliteView.

**System Contact and Location:** This information is helpful for identifying the person administratively responsible for the switch and for identifying the locations of individual switches.

**MAC Age Interval:** The number of seconds a MAC address the switch has learned remains in the switch's address table before being aged out (deleted). Aging out occurs when there has been no traffic from the device belonging to that MAC address for the configured interval.

**Time Zone:** The number of minutes your time zone location is to the West (+) or East (-) of Coordinated Universal Time (formerly GMT). The default **0** means no time zone is configured.

**Daylight Time Rule:** Specifies the daylight savings time rule to apply for your location. The default is **None**. (For more on this topic, see appendix D, "Daylight Savings Time on the SMC6624M.")

**Time:** Used in the CLI to specify the time of day, the date, and other system parameters.



## Menu: Viewing and Configuring System Information

To access the system information parameters:

1. From the Main Menu, Select...
   **3. Switch Configuration...**
   **1. System Information**

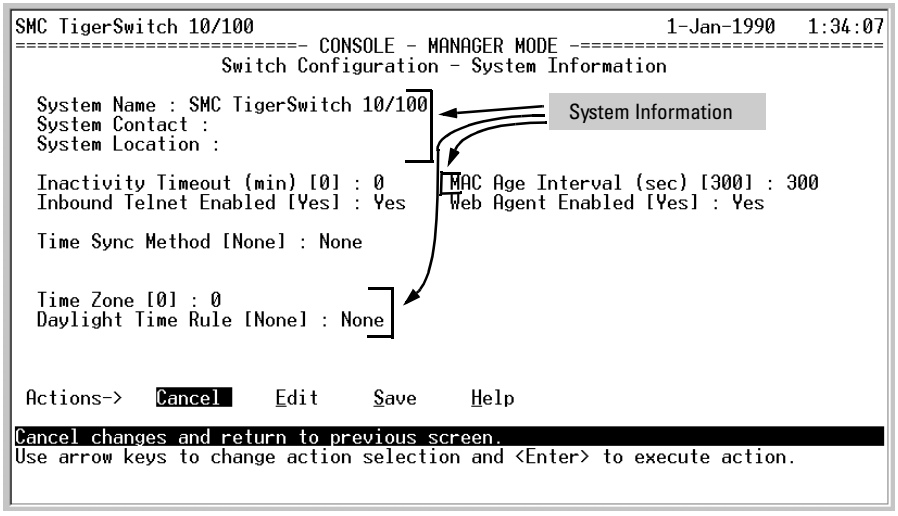



**Figure 5-8. The System Information Configuration Screen (Default Values)**

**Note**

To help simplify administration, it is recommended that you configure **System Name** to a character string that is meaningful within your system.

2. Press [E] (for Edit). The cursor moves to the **System Name** field.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press [Enter], then press [S] (for **Save**) and return to the Main Menu.

# CLI: Viewing and Configuring System Information

**System Information Commands Used in This Section**

| | |
|---|---|
| show system-information | below |
| hostname | below |
| snmp-server [contact] [location] | below |
| mac-age-time | page 5-23 |
| time timezone | page 5-23 |
| time daylight-time-rule | page 5-23 |
| time (date and time) | page 5-24 |

**Listing the Current System Information.** This command lists the current system information settings.

***Syntax***: show system-information

This example shows the switch's default console configuration.

```
Status and Counters - General System Information

 System Name         : SMC TigerSwitch 10/100
 System Contact      :
 System Location     :

 MAC Age Interval (sec) : 300

 Time Zone           : 0
 Daylight Time Rule  : None
```

**Figure 5-9. Example of CLI System Information Listing**

**Configure a System Name, Contact, and Location for the Switch.** To help distinguish one switch from another, configure a plain-language identity for the switch.

***Syntax:*** hostname *<name-string>*
snmp-server [contact *<system contact>*] [location *<system location>*]

Note that *no blank spaces* are allowed in the variables for these commands.

For example, to name the switch "Blue" with "Ext-3002" as the system contact, and "North-Data-Room" as the location:

```
SMC TigerSwitch 10/100(config)# hostname Blue
Blue(config)# snmp-server contact Ext-3002 location North-Data-Room
Blue(config)# show system-information
```

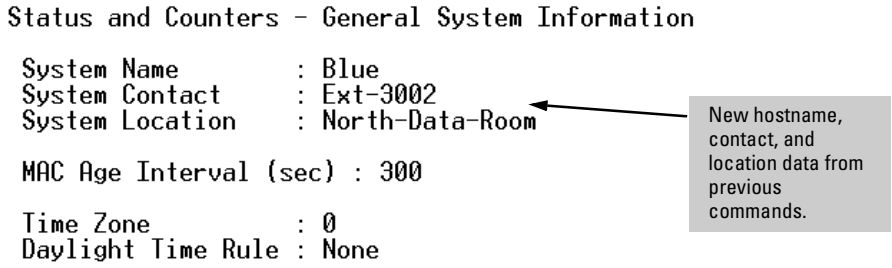



**Figure 5-10. System Information Listing After Executing the Preceding Commands**

**Reconfigure the Age Interval for Learned MAC Addresses.** This command corresponds to the MAC Age Interval in the menu interface, and is expressed in seconds.

***Syntax:*** mac-age-time *<10 . . 1000000>* (seconds)

For example, to configure the age interval to seven minutes:

```
SMC TigerSwitch 10/100(config)# mac-age-time 420
```

**Configure the Time Zone and Daylight Time Rule.** These commands:

- Set the time zone you want to use
- Define the daylight time rule for keeping the correct time when daylight-saving-time shifts occur.

***Syntax:*** time timezone <1440 . . -1440>
time daylight-time-rule <none | alaska | continental-us-and-canada | middle-europe-and-portugal | southern-hemisphere | western-europe | user-defined>

For example, this command configures the time zone and daylight time rule for Vancouver, British Columbia in Canada (time zone 8 = 480 minutes):

```
SMC TigerSwitch 10/100(config)# time timezone 480 day-
light-time-rule
       continental-us-and-canada
```

**Configure the Time and Date.** The switch uses the time command to configure both the time of day and the date. Also, executing time without parameters lists the switch's time of day and date. Note that the CLI uses a 24-hour clock scheme; that is, hour (*hh*) values from 1 p.m. to midnight are input as 13 - 24, respectively.

***Syntax:*** time [*hh:mm*[:*ss*]] [*mm/dd/*[*yy*]*yy*]

For example, to set the switch to 3:45 p.m. on October 1, 2000:

```
SMC TigerSwitch 10/100(config)# time 15:45 10/01/00
```

**Note**

Executing **reload** or **boot** resets the time and date to their default startup values.

## Web: Configuring System Parameters

In the web browser interface, you can enter the following system information:

- System Name
- System Location
- System Contact

For access to the MAC Age Interval and the Time parameters, use the menu interface or the CLI.

**Configure System Parameters in the Web Browser Interface.**

1. Click on the **Configuration** tab.
2. Click on [System Info].
3. Enter the data you want in the displayed fields.
4. Implement your new data by clicking on [Apply Changes].

# Optimizing Port Usage Through Traffic Control and Port Trunking

## Overview

This chapter includes:

- Configuring ports, including mode (speed and duplex), flow control, and broadcast control parameters (page 6-1)
- Creating and modifying a dynamic LACP or static port trunk group (page 6-9)

Port numbers in the status and configuration screens correspond to the port numbers on the front of the switch.



## Viewing Port Status and Configuring Port Parameters

**Port Status and ConfigurationFeatures**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port status | n/a | page 6-4 | page 6-5 | page 6-8 |
| configuring ports | 10/100TX, Enabled, Auto | page 6-4 | page 6-7 | page 6-8 |

**Table 6-1. Status and Parameters for Each Port Type**

| Status or Parameter | Description |
|---|---|
| Intrusion Alert (read-only) | **Yes:** The switch has detected an attempt by an unauthorized device to communicate through the indicated port.<br>**No:** Either no unauthorized devices have been detected on the port, or any detected violations have been cleared.<br>*For more on intrusions and intrusion alerts, see "Configuring and Monitoring Port Security" on page 7-7.* |
| Enabled | **Yes** (default): The port is ready for a network connection.<br>**No:** The port will not operate, even if properly connected in a network. Use this setting, for example, if the port needs to be shut down for diagnostic purposes or while you are making topology changes. |
| Status (read-only) | **Up**: The port senses a linkbeat.<br>**Down**: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, see the *Installation Guide* you received with the switch. See also chapter 11, "Troubleshooting" (in this manual). |
| Mode | The port's speed and duplex (data transfer operation) setting.<br>10/100Base-T ports:<br>• Auto (default): Senses speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex).<br>**Note:** Ensure that the device attached to the port is configured for the same setting that you select here. Also, if "Auto" is used, the device to which the port is connected must operate in compliance with the IEEE 802.3u "Auto Negotiation" standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, or is not set to Auto, then the port configuration on the switch must be manually set to match the port configuration on the other device.<br>To see what the switch negotiates for the Auto setting, use the CLI **show interfaces** command or the " **3. Port Status"** option under **"1. Status and Counters"** in the menu interface.<br>• Auto-10: Allows the port to negotiate between half-duplex (HDx) and full-duplex (FDx) while keeping speed at 10 Mbps. Also negotiates flow control (enabled or disabled). SMC recommends Auto-10 for links between 10/100 autosensing ports connected with Cat 3 cabling. (Cat 5 cabling is required for 100 Mbps links.).<br>• 10HDx:10 Mbps, Half-Duplex<br>• 10FDx: 10 Mbps, Full-Duplex<br>• 100HDx: 100 Mbps, Half-Duplex<br>• 100FDx: 100 Mbps, Full-Duplex<br>100FX ports:<br>• 100HDx (default): 100 Mbps, Half-Duplex<br>• 100FDx: 100 Mbps, Full-Duplex |

| Status or Parameter | Description |
|---|---|
| | 100/1000Base-T ports:<br>• Auto (default): Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI).<br>To see what the switch negotiates for the Auto setting, use the CLI **show interfaces** command or the " **3. Port Status"** option under "**1. Status and Counters"** in the menu interface.<br>• 1000Fdx: 1000 Mbps (1Gbps), Full-Duplex only<br>• 100Fdx: 100 Mbps, Full-Duplex<br>**Notes:**<br>• Changing the port speed on a transceiver port requires a reboot of the switch.<br>• Ensure that the device attached to the port is configured for the same setting that you select here. Also, if "Auto" is used, the device to which the port is connected must also be configured to "Auto" and operate in compliance with the IEEE 802.3ab "Auto Negotiation" standard for 1000Base-T networks. |
| | Gigabit fiber-optic ports (1000Base-SX and 1000Base-LX):<br>• 1000FDx (default): 1000 Mbps (1 Gbps), Full Duplex only<br>• Auto: The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port. |
| Flow Control | • Disabled (default): The port will not generate flow control packets and drops received flow control packets.<br>• Enabled: The port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.<br>With the port mode set to Auto (the default) and Flow Control enabled, the switch negotiates Flow Control on the indicated port. If the port mode is not set to Auto, or if Flow Control is disabled on the port, then Flow Control is not used. |
| Bcast Limit | Specifies the theoretical maximum of network bandwidth percentage that can be used for broadcast and multicast traffic. Any broadcast or multicast traffic exceeding that limit will be dropped. Zero (0) means the feature is disabled.<br>**Note:** If broadcast limits are configured on a group of ports, and those ports are later configured as a trunk, then the broadcast limit for the trunk will be the highest limit that was previously configured on the individual ports in the trunk. |
| Group (menu) or Trunk Group (CLI) | Menu Interface: Specifies the static trunk group, if any, to which a port belongs.<br>CLI: Appears in the **show lacp** command output to show the LACP trunk, if any, to which a port belongs.<br>**Note:** An LACP trunk requires a full-duplex link. In most cases, SMC recommends that you leave the port Mode setting at Auto (the default). See the LACP Note on page 6-10.<br>*For more on port trunking, see "Port Trunking" on page 6-9.* |
| Type | This parameter appears in the CLI **show trunk** listing and, for a port in a trunk group, specifies the type of trunk group. The default Type is passive LACP, which can be displayed by using the CLI **show lacp** command.<br>*For more on port trunking, see "Port Trunking" on page 6-9.* |

# Menu: Viewing Port Status and Configuring Port Parameters

From the menu interface, you can configure and view all port parameter settings and view all port status indicators.

**Using the Menu To View Port Status.** The menu interface displays the status for ports and (if configured) a trunk group.

From the Main Menu, select:

**1. Status and Counters . . .**

**3. Port Status**

In this example, ports 5 and 6 have previously been configured as a trunk group.

```
=========================- CONSOLE - MANAGER MODE -============================
                        Status and Counters - Port Status

                      Intrusion                                  Flow     Bcast
  Port      Type        Alert     Enabled  Status     Mode        Ctrl     Limit
 -------  --------  ---------  -------  ------  ----------  ---------  ------
  1        10/100TX  No         Yes      Down    10HDx       off        0
  2        10/100TX  No         Yes      Up      100FDx      off        0
  3        10/100TX  No         Yes      Up      100FDx      off        0
  4        10/100TX  No         Yes      Up      100FDx      off        0
  5-Trk1   10/100TX  No         Yes      Up      100FDx      off        0
  6-Trk1   10/100TX  No         Yes      Up      100FDx      off        0
  7        10/100TX  No         Yes      Up      10HDx       off        0
  8        10/100TX  No         Yes      Up      10HDx       off        0

 Actions->   Back     Intrusion log     Help                100FDx

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 6-11. Example of the Port Status Screen**

**Using the Menu To Configure Ports.**

**Note**

The menu interface uses the same screen for configuring both individual ports and port trunk groups. For information on port trunk groups, see “Port Trunking” on page 6-9.

1. From the Main Menu, Select:

   **2. Switch Configuration...**

   **2. Port/Trunk Settings**

```
============================- CONSOLE - MANAGER MODE -=============================
                    Switch Configuration - Port/Trunk Settings

  Port    Type       Enabled      Mode       Flow Ctrl  Group    Type
  ----  ---------  + -------  ------------  ---------  -----  --------
  1     10/100TX   | Yes      Auto          Disable
  2     10/100TX   | Yes      Auto          Disable
  3     10/100TX   | Yes      Auto          Disable
  4     10/100TX   | Yes      Auto          Disable
  5     10/100TX   | Yes      Auto          Disable    Trk1   Trunk
  6     10/100TX   | Yes      Auto          Disable    Trk1   Trunk
  7     10/100TX   | Yes      Auto          Disable    Trk1   Trunk
  8     10/100TX   | Yes      Auto          Disable    Trk1   Trunk

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 6-12. Example of Port/Trunk Settings with a Trunk Group Configured**

2. Press [E] (for Edit). The cursor moves to the **Enabled** field for the first port.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press [Enter], then press [S] (for **Save**).

## CLI: Viewing Port Status and Configuring Port Parameters

### Port Status and Configuration Commands

| | |
|---|---|
| show interfaces | below |
| show interface config | page 6-6 |
| interface | page 6-7 |

From the CLI, you can configure and view all port parameter settings and view all port status indicators.

**Using the CLI To View Port Status.** Use the following commands to display port status and configuration:

- **show interfaces**: Lists the full status and configuration for all ports on the switch.
- **show interface config**: Lists a subset of the data shown by the **show interfaces** command (above); that is, only the enabled/disabled, mode, and flow control status for all ports on the switch.

***Syntax:*** show interfaces
show interface config

The next two figures list examples of the output of the above two commands for the same port configuration on the SMC6624M.

```
SMC TigerSwitch 10/100> show interfaces

 Status and Counters - Port Status

                  | Intrusion                                Flow      Bcast
  Port Type       | Alert     Enabled Status Mode           Ctrl      Limit
  ---- --------- + --------- ------- ------ ---------- --------- ------
  1    10/100TX   | No        Yes     Down   10HDx        off       0
  2    10/100TX   | No        Yes     Down   10HDx        off       0
  3    10/100TX   | No        Yes     Down   10HDx        off       0
  4    10/100TX   | No        Yes     Down   10HDx        off       0
  5    10/100TX   | No        Yes     Down   10HDx        off       0
  6    10/100TX   | No        Yes     Down   10HDx        off       0
  7    10/100TX   | No        Yes     Down   10HDx        off       0
  8    10/100TX   | No        Yes     Down   10HDx        off       0
```

**Figure 6-1. Example of a Show Interface Command Listing**

```
SMC TigerSwitch 10/100> show interface config

 Port Settings

  Port Type       | Enabled Mode          Flow Ctrl
  ---- --------- + ------- ------------ ---------
  1    10/100TX   | Yes     Auto         Disable
  2    10/100TX   | Yes     Auto         Disable
  3    10/100TX   | Yes     Auto         Disable
  4    10/100TX   | Yes     Auto         Disable
  5    10/100TX   | Yes     Auto         Disable
  6    10/100TX   | Yes     Auto         Disable
  7    10/100TX   | Yes     Auto         Disable
  8    10/100TX   | Yes     Auto         Disable
```

**Figure 6-2. Example of a Show Interface Config Command Listing**

**Using the CLI To Configure Ports.** You can configure one or more of the following port parameters. For details on each option, see Table 6-1 on page 6-2.

***Syntax:*** [no] interface <[ethernet] *port-list*>
[disable | enable]
[speed-duplex
<auto-10 |10-full | 10-half | 100-full | 100-half |auto|1000-full |>]
[flow-control]
[broadcast-limit <0 - 99>]

Note that in the above syntax you can subsitute an "**int**" for "**interface**" and an "**e**" for "**ethernet**"; that is **int e <*port-list*>**.

For example, to configure ports 1 through 4 and port 7 for 100Mbps full-duplex with a broadcast limit of 20%, you would enter this command:

```
SMC TigerSwitch 10/100(config)# int e 1-4,7  speed-duplex
100-full
   broadcast-limit 20
```

Similarly, to configure a single port with the settings in the above command, you could either enter the same command with only the one port identified, or go to the *context level* for that port and then enter the command. For example, to enter the context level for port 7 and then configure that port for 100FDx with a broadcast limit of 20%:

```
SMC TigerSwitch 10/100(config)# int e 7
SMC TigerSwitch 10/100(eth-7)# speed-duplex 100-full
broadcast-limit 20
```

If port 8 was disabled, and you wanted to enable it and configure it for 100FDx with a broadcast limit of 20%, with flow-control active and a broadcast limit of 20%, you could do so with either of the following command sets.

- This command enables and configures port 8 from the config level:

  ```
  SMC TigerSwitch 10/100(config)# interface e 8 enable
  speed-duplex
  100-full broadcast-limit 20 flow-control
  ```

- These two commands select the context level for port 8 and then apply all of the configuration commands to port 8:

  ```
  SMC TigerSwitch 10/100(config)# int e 8
  SMC TigerSwitch 10/100(eth-8)# enable speed-duplex
  100-full
  flow-control broadcast-limit 20
  ```

## Web: Viewing Port Status and Configuring Port Parameters

In the web browser interface:

1. Click on the **Configuration** tab.
2. Click on [Port Configuration].
3. Select the ports you want to modify and click on [Modify Selected Ports].
4. After you make the desired changes, click on [Apply Settings].

Note that the web browser interface displays an existing port trunk group. However, to configure a port trunk group, you must use the CLI or the menu interface. For more on this topic, see “Port Trunking” on page 6-9.

# Port Trunking

### Port Status and ConfigurationFeatures

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port trunks | n/a | page 6-15 | page 6-17 | page 6-22 |
| configuring a static trunk group | none | page 6-15 | page 6-20 | — |
| configuring a dynamic LACP trunk group | LACP passive | — | page 6-21 | — |



Port trunking allows you to assign up to four physical links to one logical link (trunk) that functions as a single, higher-speed link providing dramatically increased bandwidth. This capability applies to connections between backbone devices as well as to connections in other network areas where traffic bottlenecks exist. A *trunk group* is a set of up to four ports configured as members of the same port trunk. Note that the ports in a trunk group do not have to be consecutive. For example:

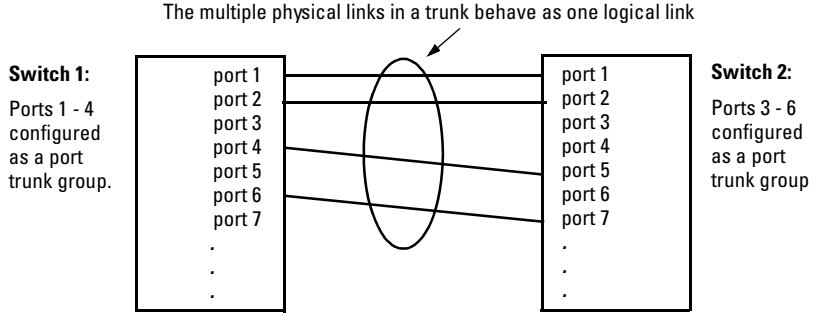



**Figure 6-3. Conceptual Example of Port Trunking**

With full-duplex operation in a four-port trunk group, trunking enables the following bandwidth capabilities:

**Table 6-2. Bandwidth Capacity for Trunk Groups Configured for Full-Duplex**

| | 10 Mbps Links | 100 Mbps Links | 1000 Mbps Links |
|---|---|---|---|
| 2 Ports | Up to 40 Mbps | Up to 400 Mbps | Up to 4000 Mbps |
| 3 Ports | Up to 60 Mbps | Up to 600 Mbps | n/a* |
| 4 Ports | Up to 80 Mbps | Up to 800 Mbps | n/a* |

* The SMC6624M offers a maximum of two gigabit links if optional gigabit transceivers are installed.

**Port Connections and Configuration:** All port trunk links must be point-to-point connections between the SMC6624M and another switch, router, server, or workstation configured for port trunking. No intervening, non-trunking devices are allowed. It is important to note that ports on both ends of a port trunk group must have the same mode (speed and duplex) and flow control settings.

**Note**

**Link Connections.** The switch does not support port trunking through an intermediate, non-trunking device such as a hub, or using more than one media type in a port trunk group. Similarly, all links in the same trunk group must have the same speed, duplex, and flow control.

**Port Security Restriction.** Port security does not operate on a trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch will reset the port security parameters for those ports to the factory-default configuration.



**Caution**

**To avoid broadcast storms or loops** in your network while configuring a trunk, first disable or disconnect all ports you want to add to or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

## SMC6624M Port Trunk Features and Operation

The SMC6624M switch offers these options for port trunking:

- LACP (IEEE 802.3ad—page 6-23)
- Trunk (non-protocol—page 6-26)
- FEC (Fast EtherChannel®—page 6-26)

The SMC6624M switch supports one trunk group of up to four ports. (Using the Link Aggregation Control Protocol—LACP—option, you can include standby trunked ports in addition to the maximum of four actively trunking ports.)

**LACP Note**

LACP operation requires full-duplex (FDx) links. For most installations, SMC recommends that you leave the port Mode settings at **Auto** (the default). LACP also operates with **Auto-10** (if negotiation selects HDx), **10FDx**, **100FDx**, and **1000FDx** settings.

**Fault Tolerance:** If a link in a port trunk fails, the switch redistributes traffic originally destined for that link to the remaining links in the trunk. The trunk remains operable as long as there is at least one link in operation. If a link is restored, that link is automatically included in the traffic distribution again. The LACP option also offers a standby link capability, which enables you to keep links in reserve for service if one or more of the original active links fails. See "Trunk Group Operation Using LACP" on page 6-23.)

## Trunk Configuration Methods

**Dynamic LACP Trunk**: The switch automatically negotiates trunked links between LACP-configured ports on separate devices, and offers one dynamic trunk option: LACP. To configure the switch to initiate a dynamic LACP trunk with another device, use the **interface ethernet** command in the CLI to set the default LACP option to **Active** on the ports you want to use for the trunk. For example, the following command sets ports 1-4 to LACP active:

```
SMC TigerSwitch 10/100(config) int e 1-4 lacp active
```

Note that the above example works if the ports are not already operating in a trunk. To change the LACP option on ports already operating as a trunk, you must first remove them from the trunk. For example, if ports 1 - 4 were LACP-active and operating in a trunk with another device, you would do the following to change them to LACP-passive:

```
SMC TigerSwitch 10/100(config)# no int e 1-4 lacp
                    Removes the ports from the trunk.
SMC TigerSwitch 10/100(config)# int e 1-4 lacp passive
                    Configures LACP  passive.
```

**Static Trunk:** The switch uses the links you configure with the Port/Trunk Settings screen in the menu interface or the **trunk** command in the CLI to create a static port trunk. The switch offers three types of static trunks: LACP, Trunk, and FEC.

**Table 6-3. Trunk Types Used in Static and Dynamic Trunk Groups**

| Trunking Method | LACP | Trunk | FEC |
|---|---|---|---|
| Dynamic | Yes | No | No |
| Static | Yes | Yes | Yes |

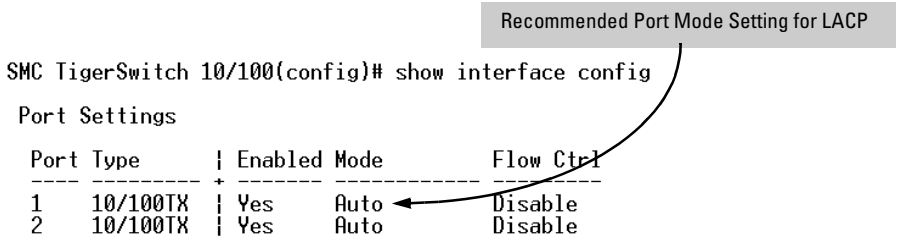
**Table 6-4. Trunk Configuration Protocols**

| Protocol | Trunking Options |
|---|---|
| LACP (802.3ad) | Provides dynamic and static LACP trunking options.<br>• **Dynamic LACP** — Use the switch-negotiated dynamic LACP trunk when:<br>– The port on the other end of the trunk link is configured for Active or Passive LACP.<br>– You want to achieve fault-tolerance for high-availability applications where you want a four-link trunk with one or more standby links available in case an active link goes down. (Both ends of the link must be dynamic LACP.)<br>• **Static LACP** — Use the manually configured static LACP trunk when:<br>– The port on the other end of the trunk link is configured for a static LACP trunk<br>– You want to configure non-default spanning tree (STP) or IGMP parameters on an LACP trunk group.<br>– You want an LACP trunk group to operate in a VLAN other than the default VLAN and GVRP is disabled.<br>– You want to use a monitor port on the switch to monitor an LACP trunk.<br><br>See "Trunk Group Operation Using LACP" on page 6-23. |
| Trunk (non-protocol) | Provides manually configured, static-only trunking to:<br>• Most switches and routing switches not running the 802.3ad LACP protocol.<br>• Windows NT and Unix workstations and servers<br>Use the Trunk option when:<br>– The device to which you want to create a trunk link is using a non-802.3ad trunking protocol<br>– You are unsure which type of trunk to use, or the device to which you want to create a trunk link is using an unknown trunking protocol.<br>– You want to use a monitor port on the switch to monitor traffic on a trunk.<br><br>See "Trunk Group Operation Using the "Trunk" Option" on page 6-26. |
| FEC | Provides static trunking to forwarding devices that also support FEC (Fast EtherChannel®), such as some Cisco® switches and routers, and some Unix and Windows NT servers.<br><br>See "Trunk Operation Using the FEC Option" on page 6-26. |

**Table 6-5. General Operating Rules for Port Trunks**

**Media:** All ports on both ends of a trunk group must have the same media type and mode (speed and duplex). The switch blocks any trunked links that do not conform to this rule. (For the SMC6624M, SMC recommends leaving the port Mode setting at **Auto** or, in networks using Cat 3 cabling, **Auto-10**.)

**Port Configuration:** The default port configuration on the SMC6624M is Auto, which enables a port to sense speed and negotiate duplex with an Auto-enabled port on another device. SMC recommends that you use the Auto setting for all ports you plan to use for trunking. Otherwise, you must manually ensure that the mode setting for each port in a trunk is compatible with the other ports in the trunk.




All of the following operate on a per-port basis, regardless of trunk membership:

- Enable/Disable
- Flow control (Flow Ctrl)
- Broadcast limit (Bcast Limit) (Note that the switch automatically adjusts the Bcast Limit setting on individual ports in the trunk to match the trunked port with the highest broadcast limit.) When a broadcast limit is configured on a trunk, removing a port from the trunk sets the broadcast limit for that port to 0 (the default).

LACP is a full-duplex protocol. See "Trunk Group Operation Using LACP" on page 6-23.

**Trunk Configuration:** All ports in the same trunk group must be the same trunk type (LACP, Trunk, or FEC). All LACP ports in the same trunk group must be either all static LACP or all dynamic LACP.

A trunk appears as a single port labeled **Dyn1** (for an LACP dynamic trunk) or **Trk1** (for a static trunk of any type: LACP, Trunk, or FEC) on various menu and CLI screens. For a listing of which screens show which trunk types, see "How the Switch Lists Trunk Data" on page 6-27.

For STP or VLAN operation, configuration for all ports in a trunk is done at the trunk level. (You cannot separately configure individual ports within a trunk for STP or VLAN operation.)

**Traffic Distribution:** All of the switch trunk protocols use the SA/DA (Source Address/Destination Address) method of distributing traffic across the trunked links. See "Outbound Traffic Distribution Across Trunked Links" on page 6-27.

**Spanning Tree Protocol (STP):** STP operates as a global setting on the switch (one instance of STP per switch). However, you can adjust STP parameters on a per-port basis. A static trunk of any type appears in the STP configuration display, and you can configure STP parameters for a static trunk in the same way that you would configure STP parameters on a non-trunked port. (Note that the switch lists the trunk by name—Trk1—and does not list the individual ports in the trunk.) For example, if ports 1 and 2 are configured as a static trunk, they are listed in the STP display as TRK1 and do not appear as individual ports in the STP displays.

In this example showing part of the **show spanning-tree** listing, ports 1 and 2 are members of TRK1 and do not appear as individual ports in the port configuration part of the listing.

```
  Port   Type       Cost  Priority State      | Designated Bridge
  ------ ---------- ----- -------- ---------- + -----------------
  3      10/100TX   10    128      Disabled   |
  4      10/100TX   10    128      Disabled   |
  5      10/100TX   10    128      Disabled   |
  6      10/100TX   10    128      Disabled   |
```

When Spanning Tree forwards on a trunk, all ports in the trunk will be forwarding. Conversely, when Spanning Tree blocks a trunk, all ports in the trunk are blocked.

**Note:** A dynamic LACP trunk operates only with the default STP settings and does not appear in the STP configuration display or **show ip igmp** listing.

If you remove a port from a static trunk, the port retains the same STP settings that were configured for the trunk.

**IP Multicast Protocol (IGMP):** A static trunk of any type appears in the IGMP configuration display, and you can configure IGMP for a static trunk in the same way that you would configure IGMP on a non-trunked port. (Note that the switch lists the trunk by name—Trk1—and does not list the individual ports in the trunk.) Also, creating a new trunk automatically places the trunk in IGMP Auto status if IGMP is enabled for the default VLAN. A dynamic LACP trunk operates only with the default IGMP settings and does not appear in the IGMP configuration display or **show ip igmp** listing.

**VLANs:** Creating a new trunk automatically places the trunk in the DEFAULT_VLAN, regardless of whether the ports in the trunk were in another VLAN. Similarly, removing a port from a trunk group automatically places the port in the default VLAN. You can configure a static trunk in the same way that you configure a port for membership in any VLAN.

**Note:** For a dynamic trunk to operate in a VLAN other than the default VLAN (DEFAULT_VLAN), GVRP must be enabled. See "Trunk Group Operation Using LACP" on page 6-23.

**Port Security:** Trunk groups (and their individual ports) cannot be configured for port security, and the switch excludes trunked ports from the **show port-security** listing. If you configure non-default port security settings for a port, then subsequently place the port in a trunk, the port security for that port returns to the default settings. If you remove a port from a trunk, the port security settings for that port are returned to their default values.

**Monitor Port:**

**Note:** A trunk cannot be a monitor port. A monitor port can monitor a static trunk but cannot monitor a dynamic LACP trunk.

# Menu: Viewing and Configuring a Static Trunk Group

**Important**

Configure port trunking *before* you connect the trunked links to another switch, routing switch, or server. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. See "Using the CLI To Configure Ports" on page 6-7.)

**To View and/or Configure Static Port Trunking:** This procedure uses the Port/Trunk Settings screen to configure a static port trunk group on the switch.

1. Follow the procedures in the Important note above.
2. From the Main Menu, Select:

   **2. Switch Configuration . . .**

   **2. Port/Trunk Settings**
3. Press [E] (for **Edit**) and then use the arrow keys to access the port trunk parameters.

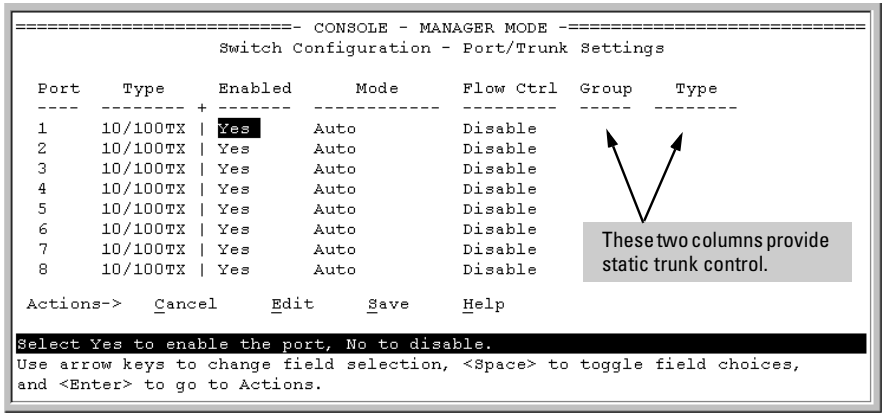



**Figure 6-4. Example of the Menu Screen for Configuring a Port Trunk Group**

4. In the Group column, move the cursor to the port you want to configure.
5. Use the Space bar to choose the **Trk1** trunk group assignment for the selected port.
   - All ports in a trunk must have the same media type and mode (such as 10/100TX set to 100FDx, or 100FX set to 100FDx). The flow control settings must also be the same for all ports in a given trunk. (The

switch automatically adjusts Broadcast Limit settings to be the same for all ports in a trunk.) To verify these settings, see "Viewing Port Status and Configuring Port Parameters" on page 6-1.

- You can configure the trunk group with one, two, three, or four ports per trunk. If multiple VLANs are configured, all ports within a trunk will be assigned to the same VLAN or set of VLANs. (With the 802.1Q VLAN capability built into the switch, more than one VLAN can be assigned to a trunk. See "Port-Based Virtual LANs (Static VLANs)" on page 9-48.)

  (To return a port to a non-trunk status, keep pressing the Space bar until a blank appears in the highlighted Group value for that port.)



```
==========================- CONSOLE - MANAGER MODE -============================
                    Switch Configuration - Port/Trunk Settings

  Port    Type      Enabled      Mode       Flow Ctrl  Group    Type
  ----  -------- + -------  ------------  ---------  -----  --------
  1     10/100TX | Yes      Auto          Disable
  2     10/100TX | Yes      Auto          Disable
  3     10/100TX | Yes      Auto          Disable
  4     10/100TX | Yes      Auto          Disable
  5     10/100TX | Yes      Auto          Disable    Trk1
  6     10/100TX | Yes      Auto          Disable    Trk1
  7     10/100TX | Yes      Auto          Disable
  8     10/100TX | Yes      Auto          Disable

 Actions->   Cancel     Edit     Save     Help

Select whether the port is part of a trunk or Mesh.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure 6-5. Example of the Configuration for a Two-Port Trunk Group**

6. Move the cursor to the Type column for the selected port and use the Space bar to select the trunk type:
   - LACP
   - Trunk (the default type if you do not specify a type)
   - FEC (Fast EtherChannel® trunk)

   All ports in the same trunk group on the same switch must have the same Type (**LACP**, **Trunk**, or **FEC**).

7. When you are finished assigning ports to the trunk group, press [Enter], then [S] (for **Save**) and return to the Main Menu. (It is not necessary to reboot the switch.)

   During the Save process, traffic on the ports configured for trunking will be delayed for several seconds. If the Spanning Tree Protocol is enabled, the delay may be up to 30 seconds.

8. Connect the trunked ports on the switch to the corresponding ports on the opposite device. If you previously disabled any of the trunked ports on the switch, enable them now. (See "Viewing Port Status and Configuring Port Parameters" on page 6-1.)

Check the Event Log (page 11-10) to verify that the trunked ports are operating properly.

# CLI: Viewing and Configuring a Static or Dynamic Port Trunk Group

**Trunk Status and Configuration Commands**

| | |
|---|---|
| show trunks | below |
| show lacp | page 6-18 |
| trunk | page 6-20 |
| interface lacp | page 6-21 |

## Using the CLI To View Port Trunks

You can list the trunk type and group for all ports on the switch or for selected ports. You can also list LACP-only status information for LACP-configured ports.

**Listing Static Trunk Type and Group for All Ports or Selected Ports.**

***Syntax:*** show trunks [*<port-list>*]

Omitting the *<port-list>* parameter results in a static trunk data listing for all LAN ports in the switch.

This example uses a port list to specify only the switch ports an administrator wants to view:

```
SMC TigerSwitch 10/100# show trunk 5-8

 Load Balancing

  Port Type       | Group Type
  ---- ---------- + ----- -----
  5    10/100TX   | Trk1  Trunk
  6    10/100TX   | Trk1  Trunk
  7    10/100TX   | Trk1  Trunk
  8    10/100TX   | Trk1  Trunk
```

**Figure 6-6. Example of a Show Trunk Listing for Specific Ports**

The show trunk command in this example does not include a port list. As a result, the listing shows static trunk group information for all switch ports.

```
SMC TigerSwitch 10/100# show trunk

 Load Balancing

  Port Type       | Group Type
  ---- ---------- + ----- -----
  1    10/100TX   |
  2    10/100TX   |
  3    10/100TX   |
  4    10/100TX   |
  5    10/100TX   | Trk1  Trunk
  6    10/100TX   | Trk1  Trunk
  7    10/100TX   | Trk1  Trunk
  8    10/100TX   | Trk1  Trunk
```

**Figure 6-7. Example of a Show Trunk Listing Without Specifying Ports**

**Listing Static LACP and Dynamic LACP Trunk Data.** This command lists data for only the LACP-configured ports.

***Syntax:*** show lacp

In the following example, ports 1, 2, and 3 have been previously configured for a static LACP trunk. (For more on "Active", see table 6-7 on page 6-24.)

```
                                LACP

PORT    LACP       TRUNK      PORT       LACP       LACP
NUMB    ENABLED    GROUP      STATUS     PARTNER    STATUS
----    -------    -------    -------    -------    -------
1       Active     Trk1       Up         Yes        Success
2       Active     Trk1       Up         Yes        Success
3       Active     Trk1       Up         Yes        Success
```

**Figure 6-8. Example of a Show LACP Listing**

**Dynamic LACP Standby Links.** Dynamic LACP trunking enables you to configure standby links for a trunk by including more than four ports in a dynamic LACP trunk configuration. When four ports (trunk links) are up, the remaining link(s) will be held in standby status. If a trunked link that is "Up" fails, it will be replaced by a standby link, which maintains your intended bandwidth for the trunk. In the next example, ports 1 through 5 have been configured for the same LACP trunk. Notice that one of the links shows Standby status, while the remaining four links are "Up".

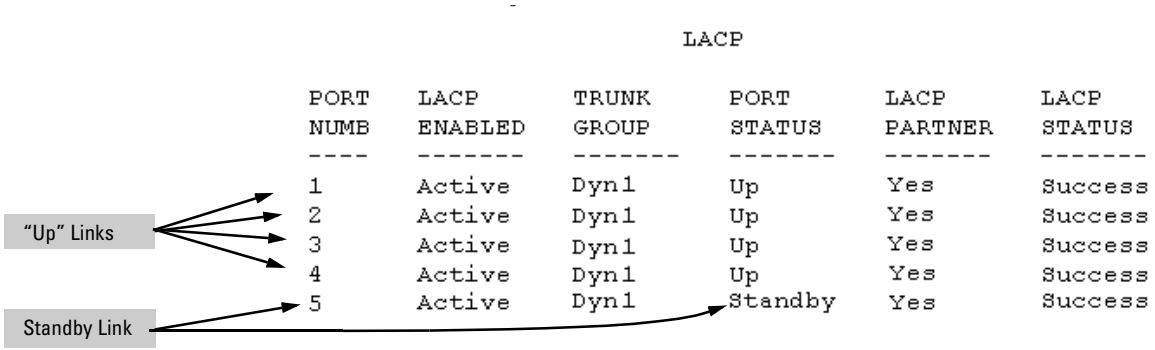



**Figure 6-9. Example of a Dynamic LACP Trunk with One Standby Link**

## Using the CLI To Configure a Static or Dynamic Trunk Group

**Important**

Configure port trunking *before* you connect the trunked links between switches. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. See "Using the CLI To Configure Ports" on page 6-7.)

On the SMC6624M, you can configure one port trunk group having up to four links (with additional standby links if you're using LACP). Options include:

- If no trunk group exists, you can create a trunk group on the switch
- If a trunk group already exists on the switch, you can add ports to the trunk group or delete ports within the group.
- You can remove a subset of ports from a trunk group, or delete the trunk group entirely by removing all ports from the group

You can configure trunk group types as follows:

| Trunk Type | Trunk Group Membership | |
|---|---|---|
| | Trk1 (Static) | Dyn1 (Dynamic) |
| LACP | Yes | Yes |
| Trunk | Yes | No |
| FEC | Yes | No |

**Note**

The following examples show how to create different types of trunk groups. However, the SMC6624M allows only one trunk group at any time.



**Configuring a Static Trunk, Static FEC, or Static LACP Trunk Group.**

***Syntax:*** trunk trk1 <trunk | fec | lacp> *<port-list>*

This example uses ports 5-8 to create a non-protocol static trunk group.

```
SMC TigerSwitch 10/100(config)# trunk trk1 trunk 5-8
```

**Removing Ports from a Static Trunk Group.** This command removes one or more ports from an existing Trk1 trunk group.

**Caution**

Removing a port from a trunk can result in a loop and cause a broadcast storm. When you remove a port from a trunk where STP is not in use, SMC recommends that you disable the port or disconnect the link on that port.

***Syntax:*** no trunk *<port-list>*

This example removes ports 7 and 8 from an existing trunk group.

```
SMC TigerSwitch 10/100(config)# no trunk 7-8
```

**Enabling a Dynamic LACP Trunk Group.** In the default port configuration, all ports on the switch are set to LACP passive. However, to enable the switch to automatically form a trunk group that is dynamic on both ends of the link, the ports on one end of a set of links must be LACP active. The ports on the other end can be either LACP active or LACP passive. This command enables the switch to automatically establish a (dynamic) LACP trunk group when the device on the other end of the link is configured for LACP passive.

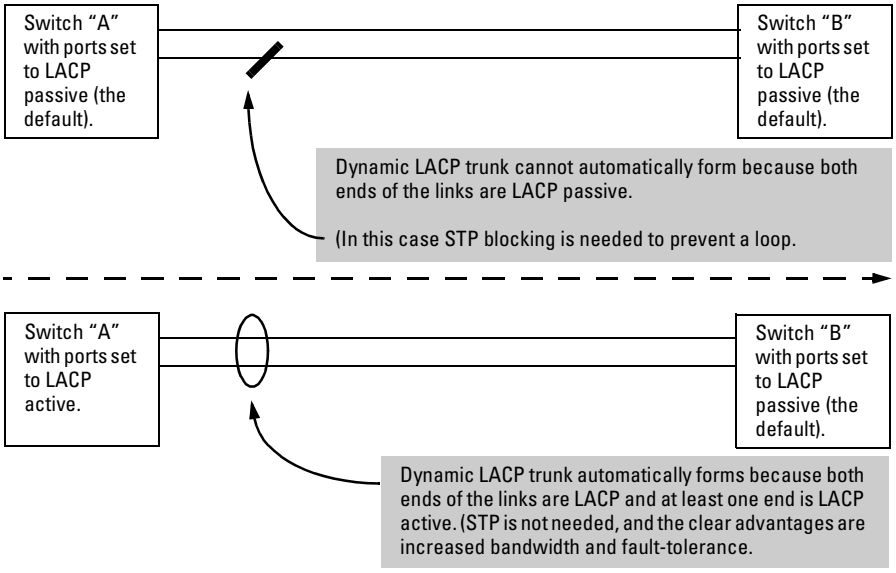



**Figure 6-10. Example of Criteria for Automatically Forming a Dynamic LACP Trunk**

***Syntax:*** interface <*port-list*> lacp active

This example uses ports 5 and 6 to enable a dynamic LACP trunk group.

```
SMC TigerSwitch 10/100(config)# interface 5-6 lacp active
```

**Removing Ports from a Dynamic LACP Trunk Group.** To remove a port from dynamic LACP trunk operation, you must turn off LACP on the port. (On a port in an operating, dynamic LACP trunk, you cannot change between LACP dynamic and LACP passive without first removing LACP operation from the port.)

**Caution**

Unless STP is running on your network, removing a port from a trunk can result in a loop. To help prevent a broadcast storm when you remove a port from a trunk where STP is not in use, SMC recommends that you first disconnect the link on that port.

***Syntax:*** `no interface` *<port-list>* `lacp`

In this example, port 1 belongs to an operating, dynamic LACP trunk. To remove port 1 from the dynamic trunk and return it to passive LACP, you would do the following:

```
SMC TigerSwitch 10/100>(config)# no interface 1 lacp
SMC TigerSwitch 10/100>(config)# interface 1 lacp passive
```

Note that in the above example, if the port on the other end of the link is configured for active LACP or static LACP, the trunked link will be re-established almost immediately.

## Web: Viewing Existing Port Trunk Groups

While the web browser interface does not enable you to configure a port trunk group, it does provide a view of an existing trunk group.

To view any port trunk groups:

Click on the **Status** tab.

Click on [Port Status].

# Trunk Group Operation Using LACP

The switch can automatically configure a dynamic LACP trunk group or you can manually configure a static LACP trunk group. The methods for displaying

**Note**

LACP requires full-duplex (FDx) links of the same media type (10/100Base-T, 100FX, etc.) and speed, and enforces speed and duplex conformance across a trunk group.

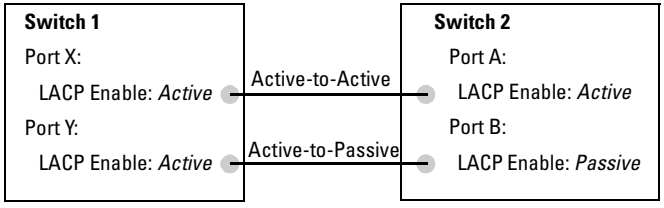
LACP trunk status include:

| Trunk Display Method | Static LACP Trunk | Dynamic LACP Trunk |
|---|---|---|
| CLI **show lacp** command | Included in listing. | Included in listing. |
| CLI **show trunk** command | Included in listing. | Not included. |
| Port/Trunk Settings screen in menu interface | Included in listing. | Not included |

In most cases, trunks configured for LACP on the SMC6624M operate as described in table 6-6:

**Table 6-6. LACP Trunk Types**

| LACP Port Trunk Configuration | Operation |
|---|---|
| Dynamic LACP | This option automatically establishes an 802.3ad-compliant trunk group, with **Dyn1** for the port Group name and **LACP** for the port Type parameter.<br>Under the following conditions, the switch automatically establishes a dynamic LACP port trunk group:<br>• The ports on both ends of a link have compatible mode settings (speed and duplex).<br>• The port on one end of a link must be configured for LACP Active and the port on the other end of the same link must be configured for either LACP Passive (the default) or LACP Active. For example: |




Either of the above link configurations allow a dynamic LACP trunk link.

**Standby Links:** A maximum of four operating links are allowed in the trunk, but, with dynamic LACP, you can configure one or more backup links that the switch automatically activates if a primary link fails. To configure a link as a standby for an existing four-port dynamic LACP trunk, ensure that both ports in the standby link are configured the same as either of the above examples.

**Displaying Dynamic LACP Trunk Data:** To list the configuration and status for a dynamic LACP trunk, use the CLI **show lacp** command.

**Note:** The dynamic trunk is automatically created by the switch, and is not listed in the static trunk listings available in the menu interface or in the CLI **show trunk** listing.

| LACP Port Trunk Configuration | Operation |
|---|---|
| Static LACP | The trunk operates if the trunk group on the opposite device is running one of the following trunking protocols:<br>• Active LACP<br>• Passive LACP<br>• Trunk<br>• FEC<br>This option uses **Trk1** for the port Group parameter and **LACP** for the port Type parameter.<br>Displaying Static LACP Trunk Data: To list the configuration and status for a static LACP trunk, use the CLI **show lacp** command. To list a static LACP trunk with its assigned ports, use the CLI **show trunk** command or display the menu interface Port/Trunk Settings screen.<br>Static LACP does not allow standby ports. |



## Default Port Operation

In the default configuration, all ports are configured for passive LACP. However, if LACP is not configured, the port will not try to detect a trunk configuration and will operate as a standard, untrunked port. The following table describes the elements of per-port LACP operation. To display this data for a particular switch, execute the following command in the CLI:

```
SMC TigerSwitch 10/100> show lacp
```

**Table 6-7. LACP Port Status Data**

| Status Name | Meaning |
|---|---|
| Port Numb | Shows the physical port number for each port configured for LACP operation (1, 2, 3 . . .). Unlisted port numbers indicate that the missing ports are assigned to a static Trunk group, an FEC trunk group, or are not configured for any trunking. |
| LACP Enabled | **Active:** The port automatically sends LACP protocol packets.<br>**Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.<br>A link having either two active LACP ports or one active port and one passive port can perform dynamic LACP trunking. A link having two passive LACP ports will not perform LACP trunking because both ports are waiting for an LACP protocol packet from the opposite device.<br>**Note:** In the default switch configuration, all ports are configured for passive LACP operation. |
| Trunk Group | **Trk1**: This port has been manually configured into a static LACP trunk.<br>**Trunk Group Same as Port Number:** The port is configured for LACP, but is not a member of a port trunk. |

| Status Name | Meaning |
|---|---|
| Port Status | **Up:** The port has an active LACP link and is not blocked or in Standby mode.<br>**Down:** The port is enabled, but an LACP link is not established. This can indicate, for example, a port that is not connected to the network or a speed mismatch between a pair of linked ports.<br>**Disabled:** The port cannot carry traffic.<br>**Blocked:** LACP, STP, or FEC has blocked the port. (The port is not in LACP Standby mode.) This may be due to a trunk negotiation (very brief) or a configuration error such as differing port speeds on the same link or attempting to connect the SMC6624M to more than one trunk.<br>**Standby:** The port is configured for dynamic LACP trunking, but the maximum number of ports for the Dyn1 trunk has already been reached on either the SMC6624M or the device on the other end of the trunked links. This port will remain in reserve, or "standby" unless LACP detects another, active link in the trunk becomes disabled, blocked, or down. In this case, LACP automatically assigns a Standby port, if available, to replace the failed port. |
| LACP Partner | **Yes:** LACP is enabled on both ends of the link.<br>**No:** LACP is enabled on the SMC6624M, but is not enabled, or LACP has not been detected on the opposite device. |
| LACP Status | **Success:** LACP is enabled on the port, detects and synchronizes with a device on the other end of the link, and can move traffic across the link.<br>**Failure:** LACP is enabled on a port and detects a device on the other end of the link, but is not able to synchronize with this device, and therefore not able to send LACP packets across the link. This can be caused, for example, by an intervening device on the link (such as a hub), a bad hardware connection, or if the LACP operation on the opposite device does not comply with the IEEE 802.3ad standard. |



## LACP Notes and Restrictions

**Changing Trunking Methods.** The switch supports one trunk group. Thus, a port belonging to an LACP dynamic trunk (Dyn1) cannot be configured as a member of a static trunk (Trk1) without first eliminating the dynamic trunk. Also, to convert a trunk from static to dynamic, you must first eliminate the static trunk.

**Static LACP Trunks.** Where a port is configured for LACP (Active or Passive), but does not belong to an existing trunk group, you can add that port to a static trunk. Doing so disables dynamic LACP on that port, which means you must manually configure both ends of the trunk.

**VLANs and Dynamic LACP.** A dynamic LACP trunk operates only in the default VLAN unless you have enabled GVRP on the switch. If you want to use LACP for a trunk on a non-default VLAN and GVRP is disabled, configure the trunk as a static trunk.

**STP and IGMP.** If spanning tree (STP) and/or IGMP is enabled in the switch, a dynamic LACP trunk operates only with the default settings for these features and does not appear in the port listings for these features.

**Half-Duplex and/or Different Port Speeds Not Allowed in LACP Trunks.** The ports on both sides of a trunk must be configured for the same speed and for full-duplex (FDx). In most cases, SMC recommends the Auto setting. The 802.3ad LACP standard specifies a full-duplex (FDx) requirement for LACP trunking.

A port configured as LACP passive and not assigned to a port trunk can be configured to half-duplex (HDx). However, in any of the following cases, a port cannot be reconfigured to an HDx setting:

- If a port is set to LACP Active, you cannot configure it to HDx.
- If a port is already a member of a static or dynamic LACP trunk, you cannot configure it to HDx.
- If a port is already set to HDx, the switch does not allow you to configure it for a static or dynamic LACP trunk.

**Dynamic/Static LACP Interoperation:** A port configured for dynamic LACP can properly interoperate with a port configured for static (Trk1) LACP, but any ports configured as standby LACP links will be ignored.

## Trunk Group Operation Using the "Trunk" Option

This method creates a trunk group that operates independently of specific trunking protocols and does not use a protocol exchange with the device on the other end of the trunk. With this choice, the switch simply uses the SA/DA method of distributing outbound traffic across the trunked ports without regard for how that traffic is handled by the device at the other end of the trunked links. Similarly, the switch handles incoming traffic from the trunked links as if it were from a trunked source.

Use the Trunk option when you are trying to establish a trunk group between the SMC6624M and another device, but the other device's trunking operation fails to interoperate properly with LACP or FEC trunking configured on the SMC6624M.

## Trunk Operation Using the "FEC" Option

This is the most flexible method for distributing traffic over trunked links when connecting to devices that use the FEC (Fast EtherChannel®) technology. FEC trunks offer the following benefits:

- Provide trunked connectivity to a FEC-compliant server, switch, or router.
- Enable quick convergence to remaining links when a failure is detected on a trunked port link.

- Depending on the capabilities of the device on the other end of the trunk, negotiate the forwarding mechanism on the trunk to the non-protocol option.
- When auto-negotiated to the SA/DA forwarding mechanism, provide higher performance on the trunk for broadcast, multicast, and flooded traffic through distribution in the same manner as non-protocol trunking.
- Support FEC automatic trunk configuration mode on other devices. That is, when connecting FEC trunks to FEC-capable servers, switches, or routers having FEC automatic trunk configuration mode enabled, the FEC trunks allow these other devices to automatically form trunk groups.



## How the Switch Lists Trunk Data

Static Trunk Group: Appears in the menu interface and the output from the CLI **show trunk** and **show interfaces** commands.

Dynamic LACP Trunk Group: Appears in the output from the CLI **show lacp** command.

| Interface Option | Dynamic LACP Trunk Group | Static LACP Trunk Group | Static Non-Protocol or FEC Trunk Group |
|---|---|---|---|
| Menu Interface | No | Yes | Yes |
| CLI **show trunk** | No | Yes | Yes |
| CLI **show interfaces** | No | Yes | Yes |
| CLI **show lacp** | Yes | Yes | No |
| CLI **show spanning-tree** | No | Yes | Yes |
| CLI **show igmp** | No | Yes | Yes |
| CLI **show config** | No | Yes | Yes |

## Outbound Traffic Distribution Across Trunked Links

All three trunk group options (LACP, Trunk, and FEC) use source-destination address pairs (SA/DA) for distributing outbound traffic over trunked links.

SA/DA (source address/destination address) causes the switch to distribute outbound traffic to the links within the trunk group on the basis of source/destination address pairs. That is, the switch sends traffic from the same source address to the same destination address through the same trunked link,

and sends traffic from the same source address to a different destination address through a different link, depending on the rotation of path assignments among the links in the trunk. Likewise, the switch distributes traffic for the same destination address but from different source addresses through different links. Because the amount of traffic coming from or going to various nodes in a network can vary widely, it is possible for one link in a trunk group to be fully utilized while others in the same trunk have unused bandwidth capacity even though the address assignments are evenly distributed across the links in a trunk. In actual networking environments, this is rarely a problem. However, if it becomes a problem, you can use the EliteView network management software available from SMC to quickly and easily identify the sources of heavy traffic (top talkers) and make adjustments to improve performance.

Broadcasts, multicasts, and floods from different source addresses are distributed evenly across the links. As links are added or deleted, the switch redistributes traffic across the trunk group. For example, in figure 6-11 showing a three-port trunk, traffic could be assigned as shown in table 6-8.

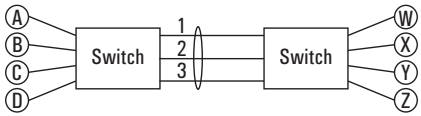



**Figure 6-11. Example of Port-Trunked Network**

**Table 6-8. Example of Link Assignments in a Trunk Group (SA/DA Distribution)**

| Source: | Destination: | Link: |
|---|---|---|
| Node A | Node W | 1 |
| Node B | Node X | 2 |
| Node C | Node Y | 3 |
| Node D | Node Z | 1 |
| Node A | Node Y | 2 |
| Node B | Node W | 3 |

# Using Passwords, Port Security, and Authorized IP Managers To Protect Against Unauthorized Access

- **Manager and Operator passwords (page 7-2):** Control access and privileges for the command line and menu interfaces (through either the console port or Telnet) and the web browser interface through the network. The features described in this chapter enhance security controls against unauthorized access through the network.
- **Port Security (page 7-7):** Enables you to specify on a per-port basis which device(s) are authorized to access the network.
- **Authorized IP Managers (page 7-28):** Enhances security on the switch by using IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This covers access through the following means:
  - Telnet
  - The switch's web browser interface
  - SNMP (with a correct community name)
  - File transfers using TFTP (for configurations and software updates)

Thus, with authorized IP managers configured, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch's Authorized IP Managers configuration.

# Using Password Security

**Password Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Set a Password | no passwords set | page 7-3 | page 7-5 | page 7-6 |
| Set User Names | no user names set | — | — | page 7-6 |
| Delete Password Protection | n/a | page 7-4 | page 7-5 | page 7-6 |

Console access includes both the menu interface and the CLI. There are two levels of console access: Manager and Operator. For security, you can set a password on each of these levels.

| Level | Actions Permitted |
|---|---|
| Manager: | Access to all console interface areas.<br>*This is the default level.* That is, if a Manager password has *not* been set prior to starting the current console session, then anyone having access to the console can access any area of the console interface. |
| Operator: | Access to the Status and Counters menu, the Event Log, and the CLI*, but no Configuration capabilities.<br>On the Operator level, the configuration menus, Download OS, and Reboot Switch options in the Main Menu are not available. |

*Allows use of the ping, link-test, show, menu, exit, and logout commands, plus the enable command if you can provide the Manager password.

To use password security:

1. Set a Manager password (and an Operator password, if applicable for your system).
2. Exit from the current console session. A Manager password will now be needed for full access to the console.

If you do steps 1 and 2, above, then the next time a console session is started for either the menu interface or the CLI, a prompt appears for a password. Assuming that both a Manager password and an Operator password have been set, the level of access to the console interface will be determined by which password is entered in response to the prompt.

If you set a Manager password, you may also want to configure the **Inactivity Time** parameter (see page 5-15). This causes the console session to end after the specified period of inactivity, thus giving you added security against unauthorized console access.

**Note** The manager and operator passwords control access to the menu interface, the CLI, and the web browser interface.

**Note** If there is only a Manager password set (with no Operator password), and the Manager password is not entered correctly when the console session begins, access to the console will be denied.

If there are both a Manager password and an Operator password, but neither is entered correctly, access to the console will be denied.

*If the switch has neither a Manager password nor an Operator password, anyone having access to the console interface can operate the console with full manager privileges. Also, if only an Operator password is set, entering the Operator password enables full manager privileges.*

Passwords are case-sensitive.

The rest of this section covers how to:

- Set Passwords
- Delete Passwords
- Recover from a Lost Password

## Menu: Setting Manager and Operator passwords

1. From the Main Menu select:

   **5. Console Passwords**

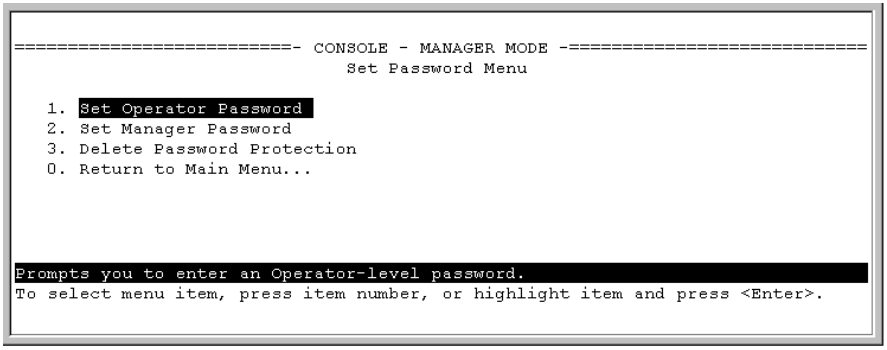



**Figure 7-1. The Set Password Screen**

2. To set a new password:
   a. Select **Set Manager Password** or **Set Operator Password**. You will then be prompted with **Enter new password**.
   b. Type a password of up to 16 ASCII characters with no spaces and press [Enter]. (Remember that passwords are case-sensitive.)
   c. When prompted with **Enter new password again**, retype the new password and press [Enter].

After a password is set, if you subsequently start a new console session, you will be prompted to enter the password.

**To Delete Password Protection (Including Recovery from a Lost Password):** This procedure deletes *both* passwords (Manager and Operator). If you have physical access to the switch, press and hold the Clear button (on the front of the switch) for a minimum of one second to clear all password protection, then enter new passwords as described earlier in this chapter. If you do not have physical access to the switch, you will need the Manager access:

1. Enter the console at the Manager level.
2. Go to the **Set Passwords** screen as described above.
3. Select **Delete Password Protection**. You will then see the following prompt:

   **Continue Deletion of password protection? No**

4. Press the Space bar to select **Yes**, then press [Enter].
5. Press [Enter] to clear the Password Protection message.

**To Recover from a Lost Manager Password:** If you cannot start a console session at the manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing and holding the Clear button for a minimum of one second. This action deletes all passwords and user names (Manager and Operator) used by both the console and the web browser interface.

## CLI: Setting Manager and Operator Passwords

**Password Commands Used in This Section**

| | |
|---|---|
| password | below |

**Configuring Manager and Operator Passwords.** This procedure prompts you to enter a password twice to help verify that you have correctly entered the desired characters.

***Syntax:*** password <manager | operator>
no password

```
SMC TigerSwitch 10/100(config)# password manager
New password: *****
Please retype new password: *****
SMC TigerSwitch 10/100(config)# password operator
New password: *****
Please retype new password: *****
```

Password entries appear as asterisks.

You must type each password entry twice.

**To Delete Password Protection.** This command prompts you to verify that you want to clear the passwords, then clears both the Manager and the Operator password.

```
SMC TigerSwitch 10/100(config)# no password
Password protection will be deleted, do you want to continue [y/n]? y
SMC TigerSwitch 10/100(config)#
```

Press (for yes) and press .

**Figure 7-2. Clearing the Manager and Operator Passwords**

## Web: Configuring User Names and Passwords

In the web browser interface you can enter both user names and passwords. Because user names do not apply in the menu interface and the CLI, they affect only your access to the switch through the web browser interface.

**To Configure (or Remove) User Names and Passwords in the Web Browser Interface.**

1. Click on the **Security** tab.

Click on [Device Passwords].

2. Do one of the following:
   - To set user name and password protection, enter the user names and passwords you want in the appropriate fields.
   - To remove user name and password protection, leave the fields blank.
3. Implement the user names and passwords by clicking on [Apply Changes].

# Configuring and Monitoring Port Security

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Displaying Current Port Security | n/a | — | page 7-14 | page 7-20 |
| Configuring Port Security | disabled | — | page 7-15 | page 7-20 |
| Intrusion Alerts and Alert Flags | n/a | page 7-25 | page 7-23 | page 7-26 |

Using Port Security, you can configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

**Note**

This feature does not prevent intruders from receiving broadcast and multicast traffic.



## Basic Operation

**Default Port Security Operation.** The default port security setting for each port is off, or "continuous." That is, any device can access a port without causing a security reaction.

**Intruder Protection.** A port that detects an "intruder" blocks the intruding device from transmitting to the network through that port.

**General Operation for Port Security.** On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as EliteView
- Alert Log entries in the switch's web browser interface
- Event Log entries in the console interface

- Intrusion Log entries in either the menu interface, CLI, or web browser interface

For any port, you can configure the following:

- **Authorized (MAC) Addresses:** Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
  - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
  - Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port. (For more on configuring the switch for SNMP management, see “Trap Receivers and Authentication Traps” on page page 8-9.)

## Blocking Unauthorized Traffic

Unless you configure the switch to disable a port on which a security violation is detected, the switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs, switches, or other devices are connected, and to maintain security while also maintaining network access to authorized users. For example:

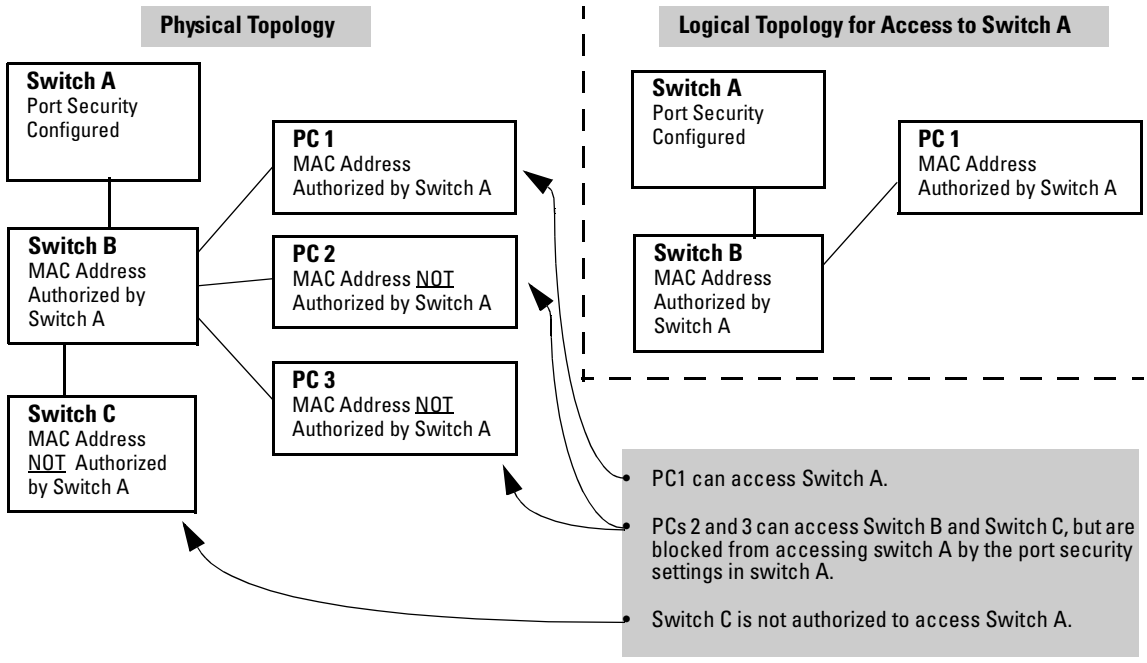



**Figure 7-3. Example of How Port Security Controls Access**

**Note**

Broadcast and Multicast traffic is not "unauthorized" traffic, and can be read by intruders connected to a port on which you have configured port security.

### Trunk Group Exclusion

Port security does not operate on either a static or dynamic trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch will reset the port security parameters for those ports to the factory-default configuration. (Ports configured for either Active or Passive LACP, and which are not members of a trunk, can be configured for port security.)

## Planning Port Security

1. Plan your port security configuration and monitoring according to the following:
   a. On which ports do you want to configure port security?

b. Which devices (MAC addresses) are authorized on each port (up to 8 per port)?

c. For each port, what security actions do you want? (The switch automatically blocks intruders detected on that port from transmitting to the network.) You can configure the switch to (1) send intrusion alarms to an SNMP management station and to (2) optionally disable the port on which the intrusion was detected.

d. How do you want to learn of the security violation attempts the switch detects? You can use one or more of these methods:
   - Through network management (That is, do you want an SNMP trap sent to a net management station when a port detects a security violation attempt?)
   - Through the switch's Intrusion Log, available through the CLI, menu, and web browser interface
   - Through the Event Log (in the menu interface or through the CLI **show log** command)

2. Use the CLI or web browser interface to configure port security operating and address controls. The following table describes the parameters.

# CLI: Port Security Command Options and Operation

**Port Security Commands Used in This Section**

| | |
|---|---|
| show port-security | page 7-14: "CLI: Displaying Current Port Security Settings" |
| port-security | page 7-15: "CLI: Configuring Port Security" |
| <[ethernet] *port-list*> | page 7-15: "CLI: Configuring Port Security" |
| [learn-mode continuous] | page 7-16: "Adding an Authorized Device to a Port" |
| [learn-mode static] | page 7-16: "Adding an Authorized Device to a Port" |
| [address-limit] | page 7-16: "Adding an Authorized Device to a Port" |
| [mac-address] | page 7-16: "Adding an Authorized Device to a Port" |
| [action] | page 7-16: "Adding an Authorized Device to a Port" |
| no port-security | page 7-18: "Removing a Device From the "Authorized" List for a Port" |
| [clear-intrusion-flag] | page 7-23: "CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags" |

This section describes the CLI port security command and how the switch acquires and maintains authorized addresses.

**Note** Use the global configuration level to execute port-security configuration commands.

**Table 7-1. Port Security Parameters**

| Parameter | Description | |
|---|---|---|
| Port List | **<[ethernet] *port-list*>** | Identifies the port or ports on which to apply a port security command. |
| Learn Mode | **learn-mode <static \| continuous>** | Specifies how the port acquires authorized addresses. |

**Continuous** (the Default)**:** Appears in the factory-default setting or when you execute **no port-security.** Allows the port to learn addresses from inbound traffic from any device(s) to which it is connected. In this state, the port accepts traaffic from any device(s) to which it is connected. Addresses learned this way appear in the switch and port address tables and age out according to the **Address Age Interval** in the System Information configuration screen (page 5-21).

**Static:** Enables you to use the **mac-address** parameter to specify the MAC addresses of the devices authorized for a port, and the **address-limit** parameter to specify the number of MAC addresses authorized for the port. You can authorize specific devices for the port, while still allowing the port to accept other, non-specified devices until the device limit has been reached. That is, if you enter fewer MAC addresses than you authorized, the port authorizes the remaining addresses in the order in which it automatically learns them. For example, If you use **address-limit** to specify three authorized devices, but use **mac-address** to specify only one authorized MAC address, the port adds the one specifically authorized MAC address to its authorized-devices list and the first two additional MAC addresses it detects. For example, suppose:

- You use **mac-address** to authorize MAC address 0060b0-880a80 for port 4.
- You use **address-limit** to allow three devices on port 4 and the port detects a series of MAC addresses in the following order:

  080090-1362f2
  00f031-423fc1
  080071-0c45a1
  0060b0-880a80 (the address you authorized with the **mac-address** parameter)

In the above case, port four would assume the following list of authorized addresses:

| | |
|---|---|
| 080090-1362f2 | (the first address the port detected) |
| 00f031-423fc1 | (the second address the port detected) |
| 0060b0-880a80 | (the address you authorized with the **mac-address** parameter) |

The remaining MAC address the port detects, 080071-0c45a1, is not allowed in the list of authorized addresses, and so is handled as an intruder.

**Permanence of Authorized Addresses In Static Mode:** A MAC address that you specifically authorize with the **mac-address** parameter cannot age-out. Instead, it remains in the port's authorized-devices list until you take one of the following actions: Remove it with a CLI command; Use the CLI to disable port security on the port; Reset the switch to its default configuration; Reboot without first executing **write memory**.

While in Static mode, if a port adds a MAC address that you have not specifically authorized (see above example), that address remains in the Authorized list until you take one of the following actions: Remove it with a CLI command; Remove the link and reboot the switch after device detection; Disable port security on that port; Reset the switch to its factory-default configuration.

**Caution:** When you use **static** with a device limit greater than the number of MAC addresses you specify with **mac-address**, an unwanted device can become "authorized". This can occur because the port, in order to fulfill the number of devices allowed by the **address-limit** parameter, automatically adds devices it detects until the specified limit is reached.

| Parameter | Description |
|---|---|
| Device Limit | **address-limit *<integer>***<br>When Learn Mode is set to **Static**, specifies how many authorized devices (MAC addresses) to allow. Range: 1 (the default) to 8. |
| Action | **action** <none \| send-alarm \| send-disable><br>Specifies whether an SNMP trap is sent to a network management station when Learn Mode is set to **static** and the port detects an unauthorized device, or when Learn Mode is set to continuous and there is an address change on a port.<br><br>**None (the default):** Prevents an SNMP trap from being sent.<br><br>**Send Alarm:** Causes the switch to send an SNMP trap to a network management station.<br><br>**Send Alarm and Disable:** Available only in the **static** learn-mode. Causes the switch to send an SNMP trap to a network management station and disable the port.<br><br>For information on configuring the switch for SNMP management, see chapter 8. |
| Address List | **mac-address *<mac-addr>***<br>Available for **static** learn mode. Allows up to eight authorized devices (MAC addresses) per port, depending on the value specified in the **address-limit** parameter.<br><br>If you use **mac-address** with **static**, but enter fewer devices than you specified in the **address-limit** field, the port accepts not only your specified devices, but also as many other devices as it takes to reach the device limit. For example, if you specify four devices, but enter only two MAC addresses, the port will accept the first two non-specified devices it detects, along with the two specifically authorized devices. |
| Clear Intrusion Flag | **clear-intrusion-flag**<br>Clears the intrusion flag for a specific port. (See "Reading Intrusion Alerts and Resetting Alert Flags" on page 7-20.) |

## CLI: Displaying Current Port Security Settings

The CLI uses the same command to provide two types of port security listings:

- All ports on the switch with their Learn Mode and (alarm) Action
- Only the specified ports with their Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses

**Using the CLI To Display Port Security Settings.**

***Syntax:*** show port-security
show port-security *<port number>*
show port-security [*<port number>*-*<port number*]. . .[,*<port number>*]

Without port parameters, show port-security displays Operating Control settings for all ports on a switch. For example:

```
Port Security
 Port Learn Mode |          Action
 ---- ---------- + ------------------------
 1    Static     | Send Alarm, Disable Port
 2    Static     | Send Alarm, Disable Port
 3    Static     | Send Alarm
 4    Static     | Send Alarm
 5    Static     | Send Alarm
 6    Static     | Send Alarm
 7    Continuous | None
 8    Continuous | None
```

**Figure 7-4. Example Port Security Listing (Ports 7 and 8 Show the Default Setting)**

With port numbers included in the command, **show port-security** displays Learn Mode, Address Limit, (alarm) Action, and Authorized Addresses for the specified ports on a switch. The following example lists the full port security configuration for a single port:

```
Port Security
 Port : 3
 Learn Mode : Static                    Address Limit : 1
 Action : Send Alarm

 Authorized Addresses
 --------------------
 00906d-fdcc00
```

**Figure 7-5. Example of the Port Security Configuration Display for a Single Port**

The following command example shows the option for entering a range of ports, including a series of non-contiguous ports. Note that no spaces are allowed in the port number portion of the command string:

```
SMC TigerSwitch 10/100(config)# show port-security 1-
3,6,8
```

## CLI: Configuring Port Security

Using the CLI, you can:

- Configure port security and edit security settings.
- Add or delete devices from the list of authorized addresses for one or more ports.
- Clear the Intrusion flag on specific ports

***Syntax:*** port-security <*port-list*>
[learn-mode continuous]
[learn-mode static]
[address-limit <*integer*>]
[mac-address <*mac-addr*>] [<*mac-addr*> . . . <*mac-addr*>]
[action <none | send-alarm | send-disable>]
[clear-intrusion-flag]

no port-security <port-list> mac-address <*mac-addr*> [<*mac-addr*> . . . <*mac-addr*>]

For information on the individual control parameters, see the Port Security Parameter tables on pages 7-12 and 7-13.

**Specifying Authorized Devices and Intrusion Responses.** This example configures port 1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) It also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
SMC TigerSwitch 10/100(config)# port-security 1 learn-
mode static action send-disable
```

The next example does the same as the preceding example, except that it specifies a MAC address of 0c0090-123456 as the authorized device instead of allowing the port to automatically assign the first device it detects as an authorized device.

```
SMC TigerSwitch 10/100(config)# port-security 1 learn-
mode static mac-address 0c0090-123456 action send-disable
```

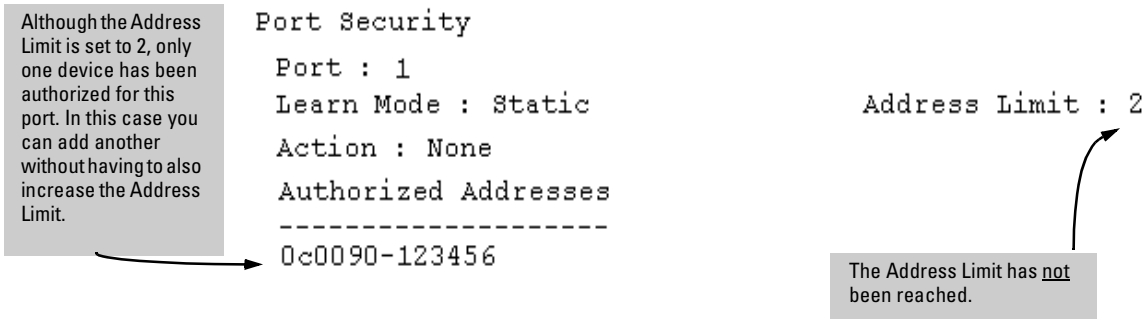
This example configures port 5 to:

- Allow two MAC addresses, 00c100-7fec00 and 0060b0-889e00, as the authorized devices
- Send an alarm to a management station if an intruder is detected on the port

```
SMC TigerSwitch 10/100(config)# port-security 5 learn-
mode static address-limit 2 mac-address 00c100-7fec00
0060b0-889e00 action send-alarm
```

If you manually configure authorized devices (MAC addresses) and/or an alarm action on a port, those settings remain unless you either manually change them or the switch is reset to its factory-default configuration. You can "turn off" authorized devices on a port by configuring the port to continuous Learn Mode, but subsequently reconfiguring the port to static Learn Mode restores those authorized devices.

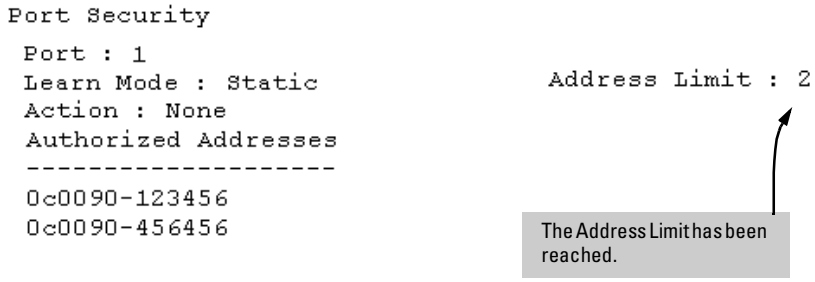
**Adding an Authorized Device to a Port.** To simply add a device (MAC address) to a port's existing Authorized Addresses list, enter the port number with the **mac-address** parameter and the device's MAC address. *This assumes that Learn Mode is set to static and the Authorized Addresses list is not full* (as determined by the current Address Limit value). For example, suppose port 2 allows two authorized devices, but has only one device in its Authorized Address list:




With the above configuration for port 1, the following command adds the 0c0090-456456 MAC address as the second authorized address.

```
SMC TigerSwitch 10/100(config)# port-security 1 mac-
address 0c0090-456456
```

After executing the above command, the security configuration for port 1 would be:




(The message `Inconsistent value` appears if the new MAC address exceeds the current Address Limit or specifies a device that is already on the list. Note that if you change a port from static to continuous learn mode, the port retains in memory any authorized addresses it had while in static mode. If you subsequently attempt to convert the port back to static mode with the same authorized address(es), the `Inconsistent value` message appears because the port already has the address(es) in its "Authorized" list.)

If you are adding a device (MAC address) to a port on which the Authorized Addresses list is already full (as controlled by the port's current Address Limit setting), then you must increase the Address Limit in order to add the device, even if you want to replace one device with another. Using the CLI, you can

simultaneously increase the limit and add the MAC address with a single command. For example, suppose port 1 allows one authorized device and already has a device listed:

```
Port Security
 Port : 1
 Learn Mode : Static                    Address Limit : 1
 Action : None
 Authorized Addresses
 --------------------
 0c0090-123456
```

To add a second authorized device to port 1, execute a port-security command for for port 1 that raises the address limit to 2 and specifies the additional device's MAC address. For example:

```
SMC TigerSwitch 10/100(config)# port-security 1 mac-
address 0c0090-456456 address-limit 2
```

**Removing a Device From the "Authorized" List for a Port.** This command option removes unwanted devices (MAC addresses) from the Authorized Addresses list. (An Authorized Address list is available for each port for which Learn Mode is currently set to "Static". See the "Address List" entry in the table on page 7-13.)

**Caution**

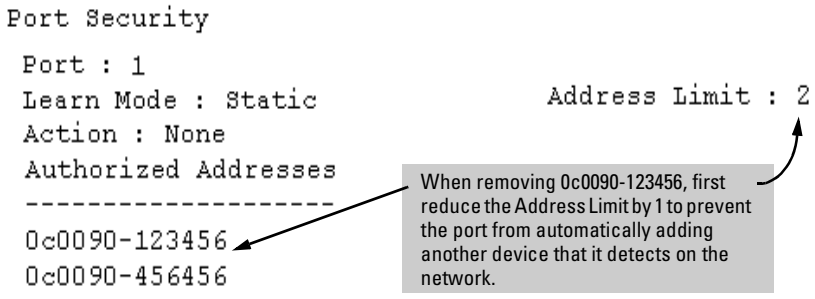
When learn mode is set to static, the Address Limit (address-limit) parameter controls how many devices are allowed in the Authorized Addresses (**mac-address**) for a given port. If you remove a MAC address from the Authorized Addresses list without also reducing the Address Limit by 1, the port may subsequently detect and accept as authorized a MAC address that you do not intend to include in your Authorized Address list. Thus, if you use the CLI to remove a device that is no longer authorized, it is recommended that you first reduce the Address Limit (**address-limit**) integer by 1, as shown below. This prevents the possibility of the same device or another unauthorized device on the network from automatically being accepted as "authorized" for that port.

To remove a device (MAC address) from the "Authorized" list and when the current number of devices equals the Address Limit value, you should first reduce the Address Limit value by 1, then remove the unwanted device.

**Note**

You can reduce the address limit below the number of currently authorized addresses on a port. This enables you to subsequently remove a device from the "Authorized" list without opening the possibility for an unwanted device to automatically become authorized.

For example, suppose port 1 is configured as shown below and you want to remove 0c0090-123456 from the Authorized Address list:




The following command serves this purpose by removing 0c0090-123456 and reducing the Address Limit to 1:

```
SMC TigerSwitch 10/100(config) # port-security 1 address-
limit 1
SMC TigerSwitch 10/100(config) # no port-security 1 mac-
address 0c0090-123456
```

The above command sequence results in the following configuration for port 1:

```
Port Security
  Port : 1
  Learn Mode : Static                Address Limit : 1
  Action : None
  Authorized Addresses
  --------------------
  0c0090-456456
```

## Web: Displaying and Configuring Port Security Features

1. Click on the **Security** tab.
2. Click on [Port Security].
3. Select the settings you want and, if you are using the Static Learn Mode, add or edit the Authorized Addresses field.
4. Implement your new data by clicking on [Apply Changes].

## Reading Intrusion Alerts and Resetting Alert Flags

### Notice of Security Violations

When the switch detects an intrusion on a port, it sets an "alert flag" for that port and makes the intrusion information available as described below. *While the switch can detect additional intrusions for the same port, it does not list the next chronological intrusion for that port in the Intrusion Log until the alert flag for that port has been reset.*

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an alert flag for that port. This flag remains set until:
  - You use either the CLI, menu interface, or web browser interface to reset the flag.
  - The switch is reset to its factory default configuration.
- The switch enables notification of the intrusion through the following means:
  - In the CLI:
    - The show intrusion-log command displays the Intrusion Log
    - The log command displays the Event Log
  - In the menu interface:
    - The Port Status screen includes a per-port intrusion alert
    - The Event Log includes per-port entries for security violations
  - In the web browser interface:
    - The Alert Log's Status | Overview window includes entries for per-port security violations
    - The Intrusion Log in the Security | Intrusion Log window lists per-port security violation entries
  - In EliteView via an SNMP trap sent to a net management station

## How the Intrusion Log Operates

When the switch detects an intrusion attempt on a port, it enters a record of this event in the Intrusion Log. No further intrusion attempts on that port will appear in the Log until you acknowledge the earlier intrusion event by resetting the alert flag.

The Intrusion Log lists the 20 most recently detected security violation attempts, regardless of whether the alert flags for these attempts have been reset. This gives you a history of past intrusion attempts. Thus, for example, if there is an intrusion alert for port 1 and the Intrusion Log shows two or more entries for port 1, only the most recent entry has not been acknowledged (by resetting the alert flag). The other entries give you a history of past intrusions detected on port 1.

```
Status and Counters - Intrusion Log
 Port  MAC Address          Date / Time
 ---- -------------- --------------------------
 1    080009-e93d4f           03/07/00 21:09:34
 1    080009-e93d4f           03/07/00 10:18:43
```

**Figure 7-6. Example of Multiple Intrusion Log Entries for the Same Port**

The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries (unless you reset the switch to its factory-default configuration). Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

## Keeping the Intrusion Log Current by Resetting Alert Flags

When a violation occurs on a port, an alert flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you reset the alert flag for either all ports or for the individual port.

## Menu: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The menu interface indicates per-port intrusions in the Port Status screen, and provides details and the reset function in the Intrusion Log screen.

1. From the Main Menu select:

   **1. Status and Counters**
   **3. Port Status**

The Intrusion Alert column shows "Yes" for any port on which a security violation has been detected.

```
=========================- CONSOLE - MANAGER MODE -============================
                      Status and Counters - Port Status

                  Intrusion                                  Flow     Bcast
  Port    Type      Alert    Enabled  Status     Mode       Ctrl     Limit
  ----  --------  ---------  -------  ------  ----------  ---------  ------
  1     10/100TX  No         Yes      Up         Auto     off        0
  2     10/100TX  No         Yes      Up         Auto     off        0
  3     10/100TX  Yes        Yes      Up         Auto     off        0
  4     10/100TX  No         Yes      Up         Auto     off        0
  5     10/100TX  No         Yes      Up         Auto     off        0
  6     10/100TX  No         Yes      Down       Auto     off        0
  7     10/100TX  No         Yes      Up         Auto     off        0
  8     10/100TX  No         Yes      Down       Auto     off        0

 Actions->   Back    Intrusion log    Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 7-7. Example of Port Status Screen with Intrusion Alert on Port 3**

2. Type [I] (**Intrusion log**) to display the Intrusion Log.

MAC Address of Intruding Device on Port 3

System Time of Intrusion on Port 3

```
=========================- CONSOLE - MANAGER MODE -============================
                      Status and Counters - Intrusion Log

  Port   MAC Address          Date / Time
  ----  -------------  -------------------------
  3     080009-6563e2          03/08/00 16:58:02
  1     0060b0-896e00          03/08/00 15:28:21
  3     080009-cf558f  prior to 03/08/00 10:28:58

 Actions->   Back    Reset alert flags    Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Indicates this intrusion on port 3 occurred prior to a reset (reboot) at the indicated time and date.

**Figure 7-8. Example of the Intrusion Log Display**

The above example shows two intrusions for port 3 and one intrusion for port 1. In this case, only the most recent intrusion at port 3 has not been acknowledged (reset). This is indicated by the following:

- Because the Port Status screen (figure 7-7 on page 7-22) does not indicate an intrusion for port 1, the alert flag for the intrusion on port 1 has already been reset.
- Since the switch can show only one uncleared intrusion per port, the older intrusion for port 3 in this example has also been previously reset.

  (The intrusion log holds up to 20 intrusion records and deletes an intrusion record only when the log becomes full and a new intrusion is subsequently detected.)

Note also that the "`prior to`" text in the record for the earliest intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

3. To acknowledge the most recent intrusion entry on port 3 and enable the switch to enter a subsequently detected intrusion on this port, type [R] (for **Reset alert flags**). (Note that if there are unacknowledged intrusions on two or more ports, this step resets the alert flags for all such ports.)

If you then re-display the port status screen, you will see that the Intrusion Alert entry for port 3 has changed to "**No**". That is, your evidence that the Intrusion Alert flag has been acknowledged (reset) is that the Intrusion Alert column in the port status display no longer shows "**Yes**" for the port on which the intrusion occurred (port 3 in this example). (Because the Intrusion Log provides a history of the last 20 intrusions detected by the switch, resetting the alert flags does not change its content. Thus, displaying the Intrusion Log again will result in the same display as in figure 7-8, above.)

## CLI: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

The following commands display port status, including whether there are intrusion alerts for any port(s), list the last 20 intrusions, and either reset the alert flag on all ports or for a specific port for which an intrusion was detected. (The record of the intrusion remains in the log. For more information, see "Operating Notes for Port Security" on page 7-26.)

| | | |
|---|---|---|
| ***Syntax:*** | show interface | List Intrusion Alert status. |
| | show intrusion-log | List Intrusion Log content. |
| | clear intrusion-log | Clear Intrusion flags on all ports. |
| | port-security <*port-number*> | |
| | clear-intrusion-flag | Clear Intrusion flag on a specific port. |

In the following example, executing show interface lists the switch's port status, which indicates an intrusion alert on port 1.

```
Status and Counters - Port Status
                 | Intrusion                                  Flow    Bcast
 Port   Type     |   Alert   Enabled Status    Mode          Ctrl    Limit
 ---- -------- + --------- ------- ------ ---------- --------- ------
 1    10/100TX | Yes        Yes     Up     10HDx      off       0
 2    10/100TX | No         Yes     Up     10HDx      off       0
 3    10/100TX | No         Yes     Up     10HDx      off       0
 4    10/100TX | No         Yes     Up     10HDx      off       0
 5    10/100TX | No         Yes     Down   10HDx      off       0
 6    10/100TX | No         Yes     Up     10HDx      off       0
 7    10/100TX | No         Yes     Up     10HDx      off       0
```

Intrusion Alert on port 1.

**Figure 7-9. Example of an Unacknowledged Intrusion Alert in a Port Status Display**

If you wanted to see the details of the intrusion, you would then enter the show intrusion-log command. For example:

```
Status and Counters - Intrusion Log
 Port  MAC Address          Date / Time
 ---- ------------- -------------------------
 1    080009-e93d4f          03/07/00 21:09:34
 1    080009-21ae84          03/07/00 17:26:27
 1    080009-e93d4f prior to 03/07/00 17:18:43
```

MAC Address of latest Intruder on Port 1

Earlier intrusions on port 1 that have already been cleared (that is, the Alert Flag has been reset at least twice before the most recent intrusion occurred.

Dates and Times of Intrusions

**Figure 7-10. Example of the Intrusion Log with Multiple Entries for the Same Port**

The above example shows three intrusions for port 1. Since the switch can show only one uncleared intrusion per port, the older two intrusions in this example have already been cleared by earlier use of the **clear intrusion-log** or the **port-security 1 clear-intrusion-flag** command. (The intrusion log holds up to 20 intrusion records, and deletes intrusion records only when the log becomes

full and new intrusions are subsequently added.) The "`prior to`" text in the record for the third intrusion means that a switch reset occurred at the indicated time and that the intrusion occurred prior to the reset.

To clear the intrusion from port 1 and enable the switch to enter any subsequent intrusion for port 1 in the Intrusion Log, execute the **port-security 1 clear-intrusion-flag** command. If you then re-display the port status screen, you will see that the Intrusion Alert entry for port 1 has changed to "**No**". That is, your evidence that the Intrusion Alert flag has been reset is the Intrusion Alert column in the port status display no longer shows "Yes" for the port on which the intrusion occurred (port 1 in this example). (Executing show intrusion-log again will result in the same display as above.)

```
SMC TigerSwitch 10/100(config)# port-security 1 clear-
intrusion-flag
SMC TigerSwitch 10/100(config)# show interface
```

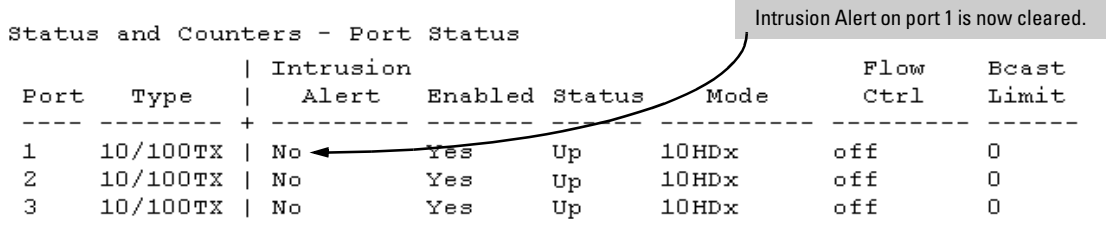



**Figure 7-11. Example of Port Status Screen After Alert Flags Reset**

## Using the Event Log To Find Intrusion Alerts

The Event Log lists port security intrusions as:

```
W MM/DD/YY HH:MM:SS FFI: port 3 — Security Violation
```

where "`W`" is the severity level of the log entry and `FFI` is the system module that generated the entry. For further information, view the Intrusion Log.

**From the CLI.** Type the log command from the Manager or Configuration level.

***Syntax:*** log *<search-text>*

For <search-text>, you can use **ffi**, **security**, or **violation**. For example:

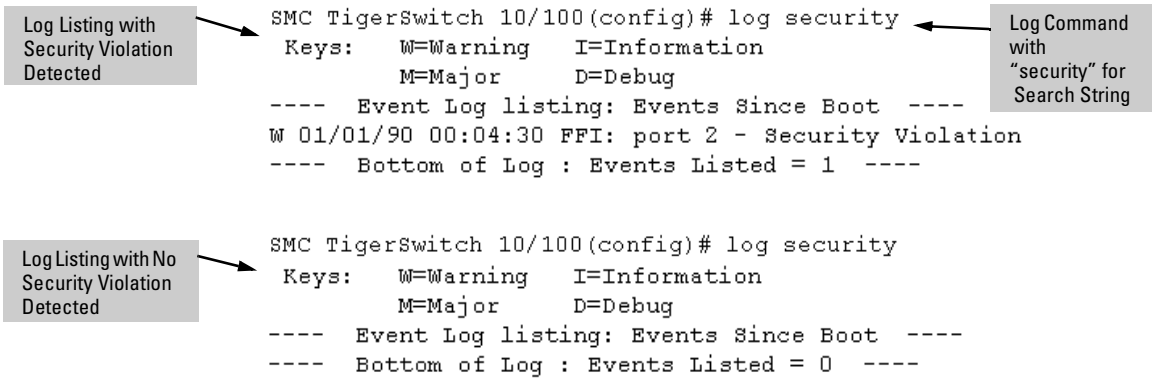



**Figure 7-12. Example of Log Listing With and Without Detected Security Violation**

**From the Menu Interface:** In the Main Menu, click on **4. Event Log** and use **Next page** and **Prev page** to review the Event Log contents.

**For More Event Log Information.** See "Using the Event Log To Identify Problem Sources" on page 11-10.

### Web: Checking for Intrusions, Listing Intrusion Alerts, and Resetting Alert Flags

1. Check the Alert Log by clicking on the **Status** tab and the [Overview] button. If there is a "Security Violation" entry, do the following:
   a. Click on the **Security** tab.
   b. Click on [Intrusion Log]. "Ports with Intrusion Flag" indicates any ports for which the alert flag has not been cleared.
   c. To clear the current alert flags, click on [Reset Alert Flags].

## Operating Notes for Port Security

**Identifying the IP Address of an Intruder.** The Intrusion Log lists detected intruders by MAC address. If you are using EliteView to manage your network, you can use reports to link MAC addresses to their corresponding IP addresses.

**Proxy Web Servers.** If you are using the switch's web browser interface through a switch port configured for Static port security, and your browser access is through a proxy web server, then it is necessary to do the following:

- Enter your PC or workstation MAC address in the port's Authorized Addresses list.
- Enter your PC or workstation's IP address in the switch's IP Authorized Managers list. See "Using IP Authorized Managers" on page 7-28.)

Without both of the above configured, the switch detects only the proxy server's MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized.

**"Prior To" Entries in the Intrusion Log.** If you reset the switch (using the Reset button, Device Reset, or Reboot Switch), the Intrusion Log will list the time of all currently logged intrusions as "prior to" the time of the reset.

**Alert Flag Status for Entries Forced Off of the Intrusion Log.** If the Intrusion Log is full of entries for which the alert flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the alert flag status for the port referenced in the dropped entry. This means that, even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the alert flags.

# Using IP Authorized Managers

**Authorized IP Manager Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Listing (Showing) Authorized Managers | n/a | page 7-31 | page 7-32 | page 7-34 |
| Configuring Authorized IP Managers | None | page 7-31 | page 7-32 | page 7-34 |
| Building IP Masks | n/a | page 7-34 | page 7-34 | page 7-34 |
| Operating and Troubleshooting Notes | n/a | page 7-37 | page 7-37 | page 7-37 |



This feature enables you to enhance security on the switch by using IP addresses to authorize which stations (PCs or workstations) can access the switch. Thus, having the correct passwords is not sufficient for accessing the switch through the network unless the station attempting access is also included in the switch's Authorized IP Managers configuration. Access controls cover:

- The switch's web browser interface
- Telnet (CLI or menu interface)
- SNMP (network management)
- File transfers using TFTP (for configurations and software updates)

You can configure:

- Up to 10 authorized manager addresses, where each address applies to either a single management station or a group of stations
- Manager or Operator access level

**Note**

This feature does not protect access to the switch through a modem or direct connection to the Console (RS-232) port. Also, if the IP address assigned to an authorized management station is configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

## Access Levels

For each authorized manager address, you can configure either of these access levels:

- **Manager:** Enables full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces.
- **Operator:** Allows view-only access from the web browser and console interfaces. (This is the same access that is allowed by the switch's operator-level password feature.)

## Defining Authorized Management Stations

- **Authorizing Single Stations:** The table entry authorizes a single management station to have IP access to the switch. To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP column, and leave the IP Mask set to **255.255.255.255**. This is the easiest way to use the Authorized Managers feature. (For more on this topic, see "Configuring One Station Per Authorized Manager IP Entry" on page 7-34.)
- **Authorizing Multiple Stations:** The table entry uses the IP Mask to authorize access to the switch from a defined group of stations. This is useful if you want to easily authorize several stations to have access to the switch without having to type in an entry for every station. All stations in the group defined by the one Authorized Manager IP table entry and its associated IP mask will have the same access level—Manager or Operator. (For more on this topic, see "Configuring Multiple Stations Per Authorized Manager IP Entry" on page 7-35.)

To configure the switch for authorized manager access, enter the appropriate *Authorized Manager IP* value, specify an *IP Mask*, and select either **Manager** or **Operator** for the *Access Level*. The IP Mask determines how the Authorized Manager IP value is used to allow or deny access to the switch by a management station.

## Overview of IP Mask Operation

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter value. ("255" in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of **255.255.255.*0*** and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 254 IP addresses for IP management access (excluding 0 for the network and 255 for broadcasts). A mask of **255.255.255.25*2*** uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses for management station access. The details on how to use IP masks are provided under "Building IP Masks" on page 7-34.

**Note**

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

# Menu: Viewing and Configuring IP Authorized Managers

From the console Main Menu, select:

**2. Switch Configuration . . .**

**7. IP Authorized Managers**

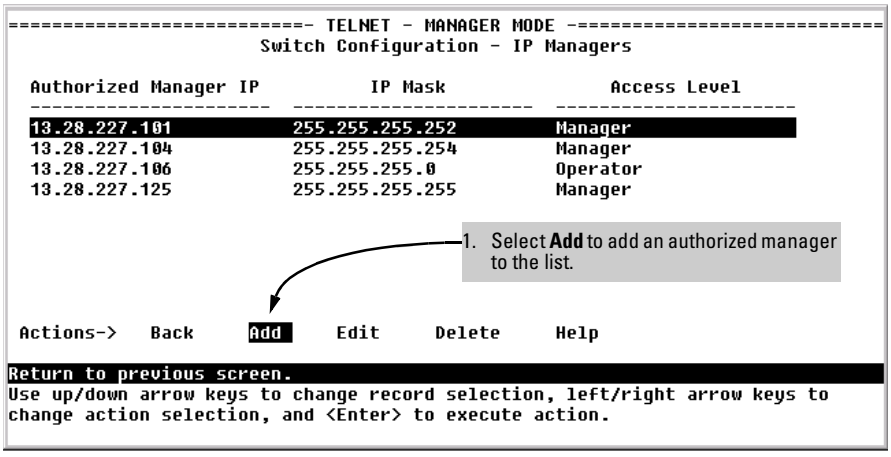



**Figure 7-13. Example of How To Add an Authorized Manager Entry**

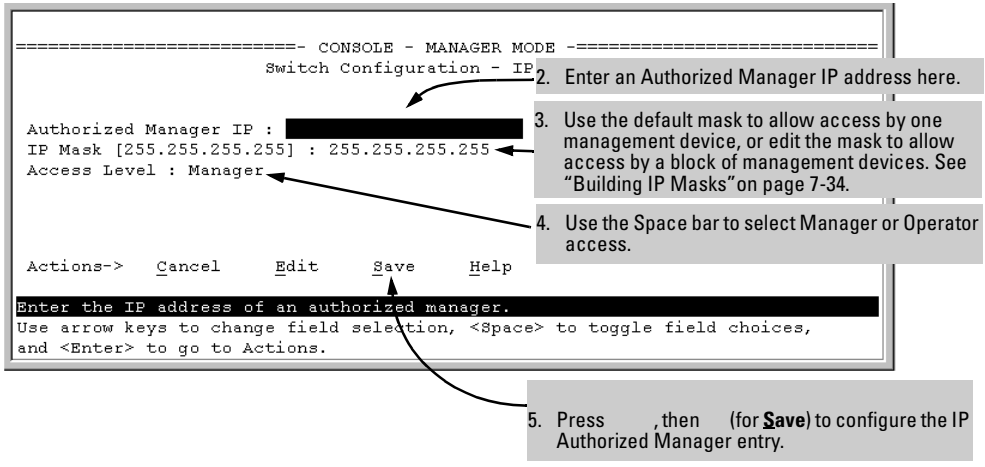



**Figure 7-14. Example of How To Add an Authorized Manager Entry (Continued)**

**Editing or Deleting an Authorized Manager Entry.** Go to the IP Managers List screen (figure 7-13), highlight the desired entry, and press [E] (for **Edit**) or [D] (for **Delete**).

## CLI: Viewing and Configuring Authorized IP Managers

**Authorized IP Managers Commands Used in This Section**

| | |
|---|---|
| show ip authorized-managers | below |
| ip authorized-managers<br>*<ip-address>*<br>mask *<mask-bits>*<br><operator \| manager> | page 7-33: "To Authorize Manager Access"<br>page 7-33: "To Edit an Existing Manager Access Entry"<br>page 7-34: "To Delete an Authorized Manager Entry" |

### Listing the Switch's Current Authorized IP Manager(s)

Use the show ip authorized-managers command to list IP stations authorized to access the switch. For example:

```
SMC TigerSwitch 10/100(config)# show ip authorized-managers
 IP Managers
  Authorized Manager IP  IP Mask                 Access Level
  ---------------------- ---------------------- -------------
  10.28.227.101          255.255.255.252        Manager
  10.28.227.104          255.255.255.254        Manager
  10.28.227.125          255.255.255.255        Manager
  10.28.227.106          255.255.255.0          Operator
```

**Figure 7-15. Example of the Show IP Authorized-Manager Display**

The above example shows an Authorized IP Manager List that allows stations to access the switch as shown below:

| IP Mask | Authorized Station IP Address: | Access Mode: |
|---|---|---|
| 255.255.255.252 | 10.28.227.100 through 103 | Manager |
| 255.255.255.254 | 10.28.227.104 through 105 | Manager |
| 255.255.255.255 | 10.28.227.125 | Manager |
| 255.255.255.0 | 10.28.227.0 *through* 255 | Operator |

## Configuring IP Authorized Managers for the Switch

***Syntax:*** ip authorized-managers *<ip address>*
[mask *<mask-bits>*]
<operator | manager>

**To Authorize Manager Access.** This command authorizes manager-level access for any station having an IP address of 10.28.227.0 through 10.28.227.255:

```
SMC TigerSwitch 10/100(config)# ip authorized-managers
   10.28.227.101 mask 255.255.255.0 manager
```

Similarly, the next command authorizes manager-level access for any station having an IP address of 10.28.227.101 through 103:

```
SMC TigerSwitch 10/100(config)# ip authorized-managers
   10.28.227.101 mask 255.255.255.252 manager
```

If you omit the mask when adding a new authorized manager, the switch automatically uses `255.255.255.255` for the mask. If you do not specify either Manager or Operator access, the switch automatically assigns the Manager access. For example:

```
SMC TigerSwitch 10/1002(config)# ip authorized-managers
   10.28.227.105
```

The result of entering the above example is:

- Authorized Station IP Address: 10.28.227.105
- IP Mask: 255.255.255.255, which authorizes only the specified station (10.28.227.105 in this case). (See "Configuring Multiple Stations Per Authorized Manager IP Entry" on page 7-35.)
- Access Level: Manager

**To Edit an Existing Manager Access Entry.** To change the mask or access level for an existing entry, use the entry's IP address and enter the new value(s). (Notice that any parameters not included in the command will be set to their default.):

```
SMC TigerSwitch 10/100(config)# ip authorized-managers
      10.28.227.101 mask 255.255.255.0 operator
```

The above command replaces the existing mask and access level for IP address 10.28.227.101 with `255.255.255.0` and `operator`.

The following command replaces the existing mask and access level for IP address 10.28.227.101 with `255.0.0.0` and `manager` (the defaults) because the command does not specify either of these parameters .

```
SMC TigerSwitch 10/100(config)# ip authorized-managers
   10.28.227.101
```

**To Delete an Authorized Manager Entry.** This command uses the IP address of the authorized manager you want to delete:

```
SMC TigerSwitch 10/100(config)# no ip authorized-managers
   10.28.227.101
```

## Web: Configuring IP Authorized Managers

In the web browser interface you can configure IP Authorized Managers as described below.

To Add, Modify, or Delete an IP Authorized Manager address:

1. Click on the **Security** tab.
2. Click on [Authorized Addresses].
3. Enter the appropriate parameter settings for the operation you want.
4. Click on [Add], [Replace], or [Delete] to implement the configuration change.

## Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

### Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them quickly by simply adding the address of each to the Authorized Manager IP list with **255.255.255.255** for the corresponding mask. For example, as shown in figure 7-15 on page 7-32, if you configure an IP address of **10.28.227.125** with an IP mask of **255.255.255.255**, only a station having an IP address of **10.28.227.125** has management access to the switch.

**Table 7-2. Analysis of IP Mask for Single-Station Entries**

| | 1st Octet | 2nd Octet | 3rd Octet | 4th Octet | Manager-Level or Operator-Level Device Access |
|---|---|---|---|---|---|
| **IP Mask** | 255 | 255 | 255 | 255 | The "255" in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 10.33.248.5. |
| **Authorized Manager IP** | 10 | 28 | 227 | 125 | |

## Configuring Multiple Stations Per Authorized Manager IP Entry

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if **255** is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than **255**).

If a bit in an octet of the mask is "on" (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is "off" (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a "255" in an IP Mask octet (*all* bits in the octet are "on") means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorized Manager IP list. A "0" (all bits in the octet are "off") means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

**Table 7-3. Analysis of IP Mask for Multiple-Station Entries**

| | 1st Octet | 2nd Octet | 3rd Octet | 4th Octet | Manager-Level or Operator-Level Device Access |
|---|---|---|---|---|---|
| **IP Mask** | 255 | 255 | 255 | 0 | The "255" in the first three octets of the mask specify that only the exact value in the octet of the corresponding IP address is allowed. However, the zero (0) in the 4th octet of the mask allows any value between 0 and 255 in that octet of the corresponding IP address. This mask allows switch access to any device having an IP address of 10.28.227.*xxx*, where *xxx* is any value from 0 to 255. |
| **Authorized Manager IP** | 10 | 28 | 227 | 125 | |
| **IP Mask** | 255 | 255 | 255 | 249 | In this example (figure 7-16, below), the IP mask allows a group of up to 4 management stations to access the switch. This is useful if the only devices in the IP address group allowed by the mask are management stations. The "249" in the 4th octet means that bits 0 and 3 - 7 of the 4th octet are fixed. Conversely, bits 1 and 2 of the 4th octet are variable. Any value that matches the authorized IP address settings for the fixed bits is allowed for the purposes of IP management station access to the switch. Thus, any management station having an IP address of 10.28.227.121, 123, 125, or 127 can access the switch. |
| **Authorized IP Address** | 10 | 28 | 227 | 125 | |



| **4th Octet of IP Mask:** | | | | **249** | | | | |
|---|---|---|---|---|---|---|---|---|
| **4th Octet of Authorized IP Address:** | | | | **5** | | | | |
| **Bit Numbers** | **Bit 7** | **Bit 6** | **Bit 5** | **Bit 4** | **Bit 3** | **Bit 2** | **Bit 1** | **Bit 0** |
| **Bit Values** | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| **4th Octet of IP Mask (249)** | ■ | ■ | ■ | ■ | ■ | □ | □ | ■ |
| **4th Octet of IP Authorized Address (125)** | □ | ■ | ■ | ■ | ■ | ■ | □ | ■ |

Bits 1 and 2 in the mask are "off", and bits 0 and 3 - 7 are "on", creating a value of 249 in the 4th octet of the mask.

Where a mask bit is "on", the corresponding bit setting in the address of a potentially authorized station must match the IP Authorized Address setting for that same bit. Where a mask bit is "off" the corresponding bit setting in the address can be either "on" or "off". In this example, in order for a station to be authorized to access the switch:

- The first three octets of the station's IP address must match the Authorized IP Address.
- Bit 0 and Bits 3 through 6 of the 4th octet in the station's address must be "on" (value = 1).
- Bit 7 of the 4th octet in the station's address must be "off" (value = 0).
- Bits 1 and 2 can be either "on" or "off".

This means that stations with the IP address 13.28.227.*X* (where *X* is 121, 123, 125, or 127) are authorized.

**Figure 7-16. Example of How the Bitmap in the IP Mask Defines Authorized Manager Addresses**

### Additional Examples for Authorizing Multiple Stations

| | Entries for Authorized Manager List | | | | Results |
|---|---|---|---|---|---|
| **IP Mask** | 255 | 255 | 0 | 255 | This combination specifies an authorized IP address of 10.33.*xxx*.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of "1" in the fourth octet of the station's IP address. |
| **Authorized Manager IP** | 10 | 33 | 248 | 1 | |
| **IP Mask** | 255 | 238 | 255 | 250 | Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet. |
| **Authorized Manager IP** | 10 | 247 | 100 | 195 | |

## Operating and Troubleshooting Notes

- **Network Security Precautions:** You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.
- **Modem and Direct Console Access:** Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.
- **Duplicate IP Addresses:** If the IP address configured in an authorized management station is also configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.
- **Web Proxy Servers:** If you use the web browser interface to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. *This reduces security by opening switch access to anyone who uses the web proxy server.* The following two options outline how to eliminate a web proxy server from the path between a station and the switch:
  - Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or "Exceptions" list in the web browser interface you are using on the authorized station.
  - If you don't need proxy server access at all on the authorized station, then just disable the proxy server feature in the station's web browser interface.

# Configuring for Network Management Applications

You can manage the switch via SNMP from a network management station. For this purpose, SMC recommends EliteView — an easy-to-install and use network management application that runs on your Windows NT- or Windows 2000-based PC. EliteView uses the RMON statistical sampling software that is included in the switch to provide powerful, but easy-to-use traffic monitoring and network activity analysis tools. For more on EliteView, see the SMC website at

**http://www.smc.com**

This chapter includes:

- An overview of SNMP management for the switch
- Configuring the SMC6624M switch for:
  - SNMP management
  - SNMP Communities
  - Trap Receivers and Authentication Traps
- Information on advanced management through RMON support

To implement SNMP management, you must either configure the switch with an appropriate IP address or, if you are using DHCP/Bootp to configure the switch, ensure that the DHCP or Bootp process provides the IP address. If multiple VLANs are configured, each VLAN interface should have its own IP network address. For DHCP use with multiple VLANs, see "Which VLAN Is Primary?" on page 9-51.

# SNMP Management Features

SNMP management features on the switch include:

- SNMP version 2c over IP
- Security via configuration of SNMP communities
- Event reporting via SNMP
  - Version 1 traps
  - RMON: groups 1, 2, 3, and 9
- Managing the switch with an SNMP network management tool such as EliteView
- Supported *Standard* MIBs include:
  - Bridge MIB (RFC 1493)
    dot1dBase, dot1dTp, dot1dStp
  - Ethernet MAU MIB (RFC 1515)
    dot3IfMauBasicGroup
  - Interfaces Evolution MIB (RFC 1573)
    ifGeneralGroup, ifRcvAddressGroup, ifStackGroup
  - RMON MIB (RFC 1757)
    etherstats, events, alarms, and history
  - SNMP MIB-II (RFC 1213)
    system, interfaces, at, ip, icmp, tcp, udp, snmp
  - Entity MIB (RFC 2037)

  *SMC Proprietary* MIBs include:
  - Statistics for message and packet buffers, tcp, telnet, and timep (netswtst.mib)
  - Port counters, forwarding table, and CPU statistics (stat.mib)
  - TFTP download (downld.mib)
  - Integrated Communications Facility Authentication Manager and SNMP communities (icf.mib)
  - SMC6624M switch configuration (config.mib)
  - SMC VLAN configuration information (vlan.mib) supporting smcVlanGeneralGroup

The switch SNMP agent also uses certain variables that are included in an SMC proprietary MIB file you can add to the SNMP database in your network management tool.

# Configuring for SNMP Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. (See "IP Configuration" on page 5-2.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See "DHCP/Bootp Operation" on page 5-10.)

Once an IP address has been configured, the general steps to configuring for SNMP access to the preceding features are:

1. From the Main menu, select

   **2. Switch Configuration . . .**

   **6. SNMP Community Names**

2. Configure the appropriate SNMP communities. (The "public" community exists by default and is used by network management applications.) (For more on configuring SNMP communities, see "Menu: Viewing and Configuring SNMP Communities" on page 8-5.)

3. Configure the appropriate trap receivers. (For more on configuring trap receivers, see "CLI: Configuring and Displaying Trap Receivers" on page 8-10.)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct community name may access the switch with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (See "Using IP Authorized Managers" on page 7-28.)

**Caution**

Deleting the community named “public” disables many network management functions (such as auto-discovery, traffic monitoring, SNMP trap generation, and threshold setting). If security for network management is a concern, it is recommended that you change the write access for the “public” community to “Restricted”.

# SNMP Communities

### SNMP Community Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| show community name | n/a | page 8-5 | page 8-7 | — |
| configure identity information | none | — | page 8-8 | |
| configure community names | public | page 8-5 | page 8-8 | — |
| MIB view for a community name (operator, manager) | manager | " | " | |
| write access for default community name | unrestricted | " | " | |

Use SNMP communities to restrict access to the switch by SNMP management stations by adding, editing, or deleting SNMP communities. You can configure up to five SNMP communities, each with either an operator-level or a manager-level view, and either restricted or unrestricted write access.

Using SNMP requires that the switch have an IP address and subnet mask compatible with your network.

**Caution**

Deleting or changing the community named “public” prevents network management applications (such as auto-discovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the switch. (Changing or deleting the “public” name also generates an Event Log message.) If security for network management is a concern, it is recommended that you change the write access for the “public” community to “Restricted”.

## Menu: Viewing and Configuring SNMP Communities

### To View, Edit, or Add SNMP Communities:

1. From the Main Menu, Select:
   **2. Switch Configuration...**
      **6. SNMP Community Names**

**Note:** This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

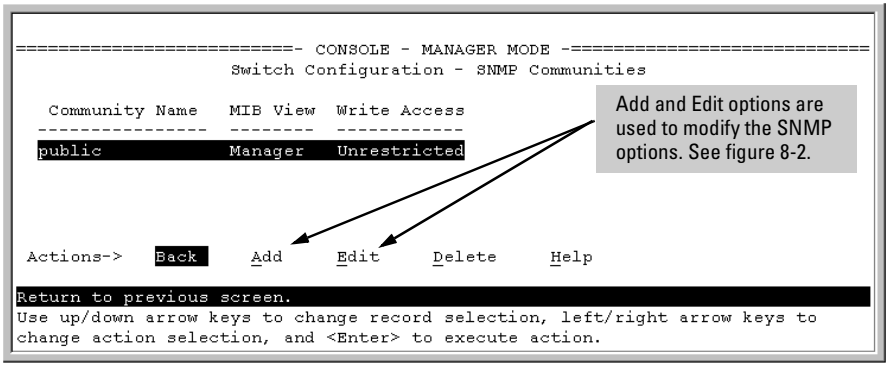



**Figure 8-1. The SNMP Communities Screen (Default Values)**

2. Press [A] (for **Add**) to display the following screen:

If you are adding a community, the fields in this screen are blank.

If you are editing an existing community, the values for the currently selected Community appear in the fields.

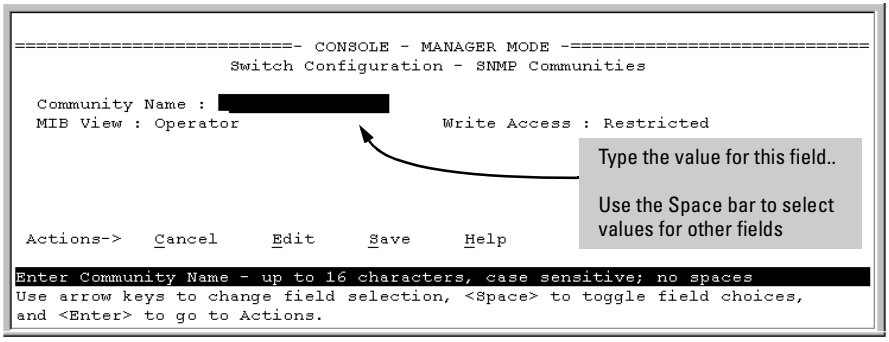



**Figure 8-2. The SNMP Add or Edit Screen**

**Need Help?** If you need information on the options in each field, press [Enter] to move the cursor to the Actions line, then select the **Help** option on the Actions line. When you are finished with Help, press [E] (for Edit) to return the cursor to the parameter fields.

3. Enter the name you want in the Community Name field, and use the Space bar to select the appropriate value in each of the other fields. (Use the [Tab] key to move from one field to the next.)

4. Press [Enter], then [S] (for **Save**).

# CLI: Viewing and Configuring Community Names

**Community Name Commands Used in This Section**

| | |
|---|---|
| show snmp-server [<*community-string*>] | below |
| snmp-server | page 8-8 |
| [contact <con*tact-str*>] | page 8-8 |
| [location <*location-str*>] | page 8-8 |
| [community <*community-str*>] | page 8-8 |
| [host <*community-str*> <*ip-addr*>] [<none \| debug \| all \| not-info \| critical>] | page 8-11 |
| [enable traps <authentication> | page 8-11 |

## Listing Current Community Names and Values

**Listing Community Names.** This command lists the data forcurrently configured SNMP community names (along with trap receivers and the setting for authentication traps — see "Trap Receivers and Authentication Traps" on page 8-9).

***Syntax***: show snmp-server [<*community-string*>]

This example lists the data for all communities in a switch; that is, both the default "public" community name and another community named "red-team."

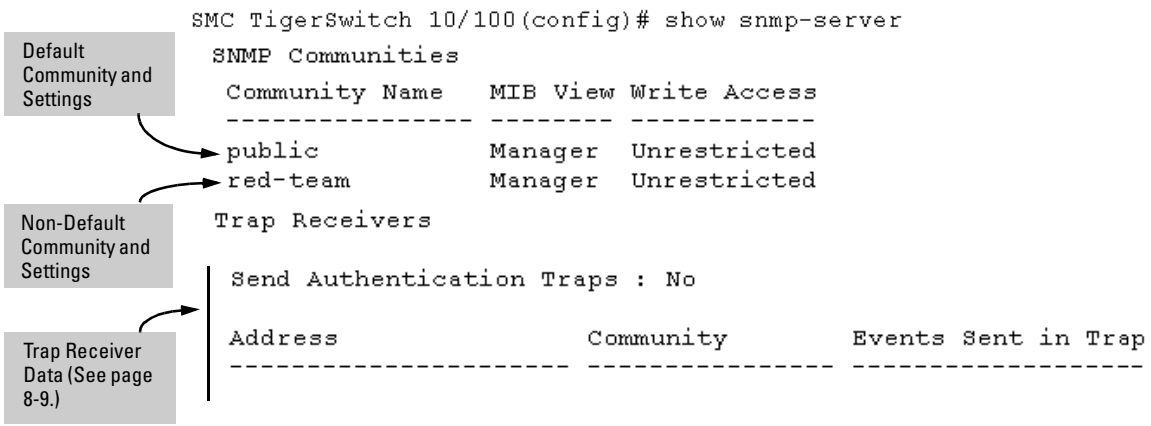



**Figure 8-3. Example of the SNMP Community Listing with Two Communities**

To list the data for only one community, such as the "public" community, use the above command with the community name included. For example:

```
SMC TigerSwitch 10/100# show snmp-server public
```

## Configuring Identity Information

This command enables you to enter contact-person and location data to help identify the switch.

***Syntax:*** snmp-server [contact <*contact-str*>] [location <*location-str*>]

Both fields allow up to 48 characters, without spaces.

For example, to configure the switch with "Site-LAN-Ext.449" and a location of "Level-2-North," you would execute the following command:

SMC TigerSwitch 10/100(config)# snmp-server contact Site-LANExt.449 location Level-2-North

## Configuring Community Names and Values

If you enter a community name without an **operator** or **manager** designation, the switch automatically assigns the community to Operator for the MIB view. Also, if you do not specify restricted or unrestricted for the read/write MIB access, the switch automatically restricts the community to read access for the MIB.

**Adding SNMP Communities in the Switch.** The following SNMP command examples use **add snmp** to add *new* SNMP communities:

***Syntax:*** snmp-server community <*community-name*>
[operator | manager]
[restricted | unrestricted]

```
SMC TigerSwitch 10/100(config)# snmp-server community
          red-team manager unrestricted
SMC TigerSwitch 10/100(config)# snmp-server community
          blue-team operator restricted
```

# Trap Receivers and Authentication Traps

### Trap Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| snmp-server host (trap receiver) | public | — | page 8-11 | — |
| snmp-server enable (authentication trap) | none | — | page 8-11 | — |

A *trap receiver* is a management station designated by the switch to receive SNMP traps sent from the switch. An *authentication trap* is a specialized SNMP trap sent to trap receivers when an unauthorized management station tries to access the switch.

**Note**

**Fixed or "Well-Known" Traps:** The SMC6624M switch automatically sends fixed traps (such as "coldStart," "warmStart," "linkDown," and "linkUp") to trap receivers using a public community name. These traps cannot be redirected to other communities. Thus, if you change or delete the default public community name, these traps will be lost.

**Thresholds:** The switch automatically sends all messages resulting from thresholds to the network management station(s) that set the thresholds, regardless of the trap receiver configuration.

In the default configuration, there are no trap receivers configured, and the authentication trap feature is disabled. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch. The switch can be configured to also send event log messages as traps if the following opotions are used with the **snmp-server host** command:

| Event Level | Description |
|---|---|
| None (default) | Send no log messages. |
| All | Send all log messages. |
| Not INFO | Send the log messages that are not information-only. |
| Critical | Send critical-level log messages. |
| Debug | Reserved for SMC-internal use. |

# CLI: Configuring and Displaying Trap Receivers

**Trap Receiver Commands Used in This Section**

| | |
|---|---|
| show snmp-server | below |
| snmp-server host *<ip-addr> <community-name>* [none \| all \| non-info\| critical \| debug] | page 8-11 |
| snmp-server enable traps authentication | page 8-11 |

## Using the CLI To List Current SNMP Trap Receivers

This command lists the currently configured trap receivers and the setting for authentication traps (along with the current SNMP community name data — see "SNMP Communities" on page 8-5).

***Syntax***: `show snmp-server`

In the next example, the **show snmp-server** command shows that the switch has been previously configured to send SNMP traps to management stations belonging to the "public," "red-team," and "blue-team" communities.

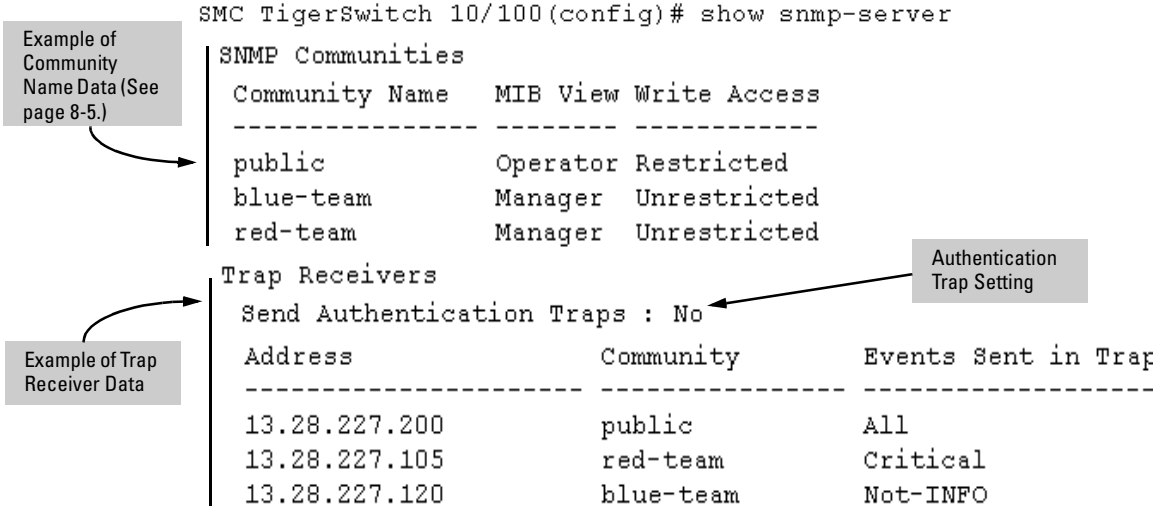



**Figure 8-4. Example of Show SNMP-Server Listing**

### Configuring Trap Receivers

This command specifies trap receivers by community membership, management station IP address, and the type of Event Log messages to send to the trap receiver.

**Note**

If you specify a community name that does not exist—that is, has not yet been configured on the switch—the switch still accepts the trap receiver assignment. However, no traps will be sent to that trap receiver until the community to which it belongs has been configured on the switch.

***Syntax:*** snmp-server host
<*community-str*> <*ip-address*> [<none | all | non-info | critical | debug>]

For example, to configure a trap receiver in a community named "red-team" with an IP address of 10.28.227.130 to receive only "critical" log messages:

```
SMC TigerSwitch 10/100(config)# snmp-server trap-receiver
red-team 10.28.227.130 critical
```

**Note**

If you do not specify the event level ([<none | all | non-info | critical | debug>]) then the switch will not send event log messages as traps. "Well-Known" traps and threshold traps (if configured) will still be sent.

## Using the CLI To Enable Authentication Traps

If this feature is enabled, an authentication trap is sent to the configured trap receiver(s) if a management station attempts an unauthorized access of the switch. Check the event log in the console interface to help determine why the authentication trap was sent. (Refer to "Using the Event Log To Identify Problem Sources" on page 11-10.)

**Note**

For this feature to operate, one or more trap receivers must be configured on the switch. See "CLI: Configuring and Displaying Trap Receivers" on page 8-10.

**Using the CLI To Enable Authentication Traps.**

***Syntax:*** snmp-server trap authentication

```
SMC TigerSwitch 10/100(config)# snmp-server trap authen-
tication
```

# Advanced Management: RMON Support

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

## RMON

The following RMON groups are supported:

- Ethernet Statistics (except the numbers of packets of different frame sizes)
- Alarm
- History (of the supported Ethernet statistics)
- Event

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events. Note that you can access the Ethernet statistics, Alarm, and Event groups from the EliteView network management software.

# Configuring Advanced Features



This chapter describes the following features and how to configure them with the switch's built-in interfaces:

- **Stack Management (Page 9-2):** Use your network to stack switches without the need for any specialized cabling.
- **Port-Based VLANs — Page 9-48:**
- **GVRP — Page 9-74:**
- **Multimedia Traffic Control with IP Multicast (IGMP) — Page 9-88:** Use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP controls.
- **Spanning Tree Protocol (STP) (Page 9-99):** Use STP to automatically block loops in your network by ensuring that there is only one active path at a time between any two nodes on the network.

For general information on how to use the switch's built-in interfaces, see:

- Chapter 2, "Using the Menu Interface"
- Chapter 3, "Using the Command Line Interface (CLI)"
- Chapter 4, "Using the Web Browser Interface
- Appendix C, "Switch Memory and Configuration"

# Stack Management

**Stacking Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| **view stack status** | | | | |
| view status of a single switch | n/a | page 9-26 thru page 9-28 | page 9-31 | page 9-46 |
| view candidate status | n/a | | page 9-31 | |
| view status of commander and its stack | n/a | | page 9-32 | |
| view status of all stacking-enabled switches in the ip subnet | n/a | | page 9-32 | |
| **configure stacking** | | | | |
| enable/disable candidate Auto-Join | enabled/Yes | page 9-15 | page 9-37 | |
| "push" a candidate into a stack | n/a | page 9-15 | page 9-38 | |
| configure a switch to be a commander | n/a | page 9-12 | page 9-33 | |
| "push" a member into another stack | n/a | page 9-24 | page 9-39 | |
| remove a member from a stack | n/a | page 9-21 | page 9-40 or page 9-41 | |
| "pull" a candidate into a stack | n/a | page 9-17 | page 9-36 | |
| "pull" a member from another stack | n/a | page 9-19 | page 9-38 | |
| convert a commander or member to a member of another stack | n/a | page 9-24 | page 9-39 | |
| access member switches for configuration and traffic monitoring | n/a | page 9-23 | page 9-42 | |
| disable stacking | enabled | page 9-15 | page 9-45 | |
| transmission interval | 60 seconds | page 9-12 | page 9-45 | |

Stack Management (termed *stacking*) enables you to use a single IP address and standard network cabling to manage a group of up to 16 SMC6624M switches in the same IP subnet (broadcast domain). Using stacking, you can:

- Reduce the number of IP addresses needed in your network.

- Simplify management of small workgroups or wiring closets while scaling your network to handle increased bandwidth demand.
- Eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technologies.
- Add SMC6624M switches to your network without having to first perform IP addressing tasks.

## Components of Stack Management

**Table 9-1. Stacking Definitions**

| | |
|---|---|
| Stack | Consists of a Commander switch and any Member switches belonging to that Commander's stack. |
| Commander | A switch that has been manually configured as the controlling device for a stack. When this occurs, the switch's stacking configuration appears as **Commander**. |
| Candidate | A switch that is ready to join (become a Member of) a stack through either automatic or manual methods. A switch configured as a Candidate is not in a stack. |
| Member | A switch that has joined a stack and is accessible from the stack Commander. |

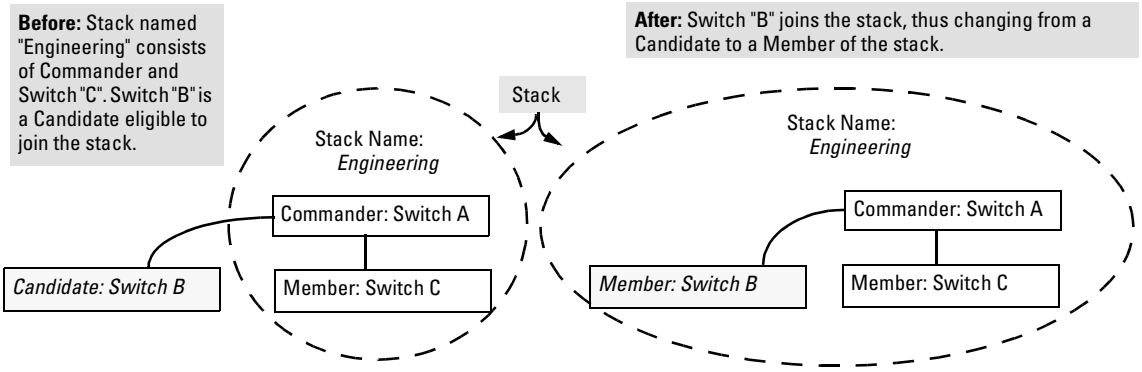



**Figure 9-1. Illustration of a Switch Moving from Candidate to Member**

## General Stacking Operation

After you configure one switch to operate as the Commander of a stack, additional switches can join the stack by either automatic or manual methods. After a switch becomes a Member, you can work through the Commander switch to further configure the Member switch as necessary for all of the additional software features available in the switch.

The Commander switch serves as the in-band entry point for access to the Member switches. For example, the Commander's IP address becomes the path to all stack Members and the Commander's Manager password controls access to all stack Members.

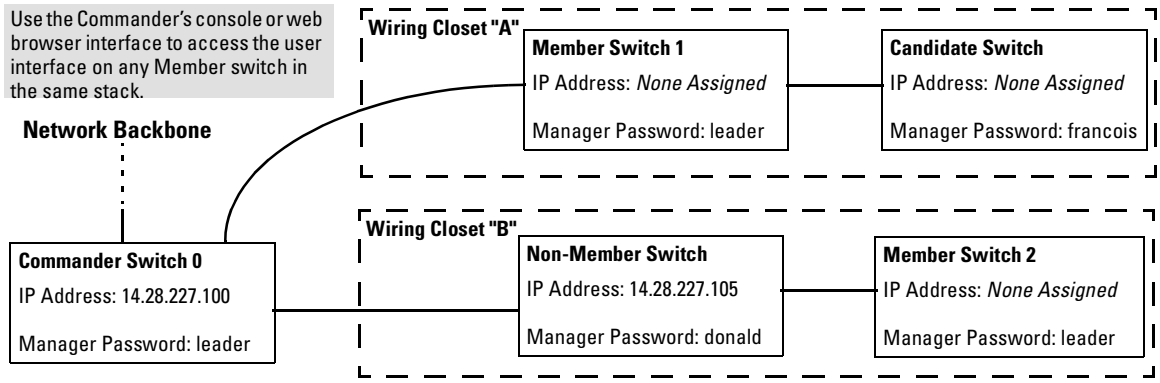



**Figure 9-2. Example of Stacking with One Commander Controlling Access to Wiring Closet Switches**

**Interface Options.** You can configure stacking through the switch's menu interface, CLI, or the web browser interface. For information on how to use the web browser interface to configure stacking, see the online Help for the web browser interface.

**Web Browser Interface Window for Commander Switches.** The web browser interface window for a Commander switch differs in appearance from the same window for non-commander switches. See figure 1-3 on page 1-4.

## Operating Rules for Stacking

### General Rules

- Stacking is an optional feature (enabled in the default configuration) and can easily be disabled. Stacking has no effect on the normal operation of the switch in your network.
- A stack requires one Commander switch. (Only one Commander allowed per stack.)
- All switches in a particular stack must be in the same IP subnet (broadcast domain). A stack cannot cross a router.
- A stack accepts up to 16 switches (numbered 0-15), including the Commander (always numbered 0).

- There is no limit on the number of stacks in the same IP subnet (broadcast domain), however a switch can belong to only one stack.
- If multiple VLANs are configured, stacking uses only the primary VLAN on any switch. In the factory-default configuration, the DEFAULT_VLAN is the primary VLAN. (See "Stacking Operation with Multiple VLANs Configured" on page 9-45 and "Which VLAN Is Primary?" on page 9-51.)
- Stacking allows intermediate devices that do not support stacking. This enables you to include switches that are distant from the Commander.

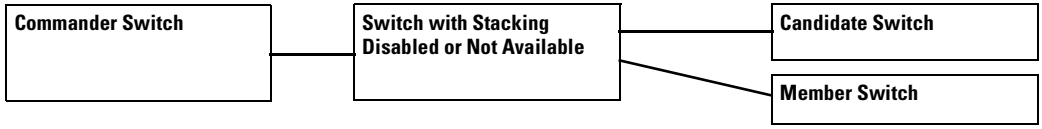



**Figure 9-3. Example of a Non-Stacking Device Used in a Stacking Environment**

## Specific Rules

Table 9-2 outlines the specific rules for switches operating in a stack.

**Table 9-2. Specific Rules for Commander, Candidate, and Member Switches**

| | IP Addressing and Stack Name | Number Allowed Per Stack | Passwords | SNMP Communities |
|---|---|---|---|---|
| Commander | **IP Addr:** Requires an assigned IP address and mask for access via the network.<br>**Stack Name:** Required | Only one Commander switch is allowed per stack. | The Commander's Manager and Operator passwords are assigned to any switch becoming a Member of the stack.<br>If you change the Commander's passwords, the Commander propagates the new passwords to all stack Members. | Standard SNMP community operation. The Commander also operates as an SNMP proxy to Members for all SNMP communities configured in the Commander. |

| | IP Addressing and Stack Name | Number Allowed Per Stack | Passwords | SNMP Communities |
|---|---|---|---|---|
| Candidate | **IP Addr:** Optional. Configuring an IP address allows access via Telnet or web browser interface while the switch is not a stack member. In the factory default configuration the switch automatically acquires an IP address if your network includes DHCP service.<br>**Stack Name:** N/A | n/a | Passwords optional. If the Candidate becomes a stack Member, it assumes the Commander's Manager and Operator passwords.<br><br>If a candidate has a password, it cannot be automatically added to a stack. In this case, if you want the Candidate in a stack, you must manually add it to the stack. | Uses standard SNMP community operation if the Candidate has its own IP addressing. |
| Member | **IP Addr:** Optional. Configuring an IP address allows access via Telnet or web browser interface without going through the Commander switch. This is useful, for example, if the stack Commander fails and you need to convert a Member switch to operate as a replacement Commander.<br>**Stack Name:** N/A | Up to 15 Members per stack. | When the switch joins the stack, it automatically assumes the Commander's Manager and Operator passwords and discards any passwords it may have had while a Candidate.<br><br>**Note:** If a Member leaves a stack for any reason, it retains the passwords assigned to the stack Commander at the time of departure from the stack. | Belongs to the same SNMP communities as the Commander (which serves as an SNMP proxy to the Member for communities to which the Commander belongs). To join other communities that *exclude* the Commander, the Member must have its own IP address. Loss of stack membership means loss of membership in any community that is configured only in the Commander. See "SNMP Community Operation in a Stack" on page 9-44. |

**Note**

In the default stack configuration, the Candidate **Auto Join** parameter is enabled, but the Commander **Auto Grab** parameter is disabled. This prevents Candidates from automatically joining a stack prematurely or joining the wrong stack (if more than one stack Commander is configured in a subnet or broadcast domain). If you plan to install more than one stack in a subnet, SMC recommends that you leave **Auto Grab** disabled on all Commander switches and manually add Members to their stacks. Similarly, if you plan to install a stack in a subnet (broadcast domain) where stacking-capable switches are not intended for stack membership, you should set the **Stack State** parameter (in the Stack Configuration screen) to **Disabled** on those particular switches.

## Overview of Configuring and Bringing Up a Stack

This process assumes that:

- All switches you want to include in a stack are connected to the same subnet (broadcast domain).
- If VLANs are enabled on the switches you want to include in the stack, then the ports linking the stacked switches must be on the primary VLAN in each switch (which, in the default configuration, is the default VLAN). If the primary VLAN is tagged, then each switch in the stack must use the same VLAN ID (VID) for the primary VLAN. (See "Which VLAN Is Primary?" on page 9-51, and "Stacking Operation with Multiple VLANs Configured" on page 9-45.)

**Options for Configuring a Commander and Candidates.** Depending on how Commander and Candidate switches are configured, Candidates can join a stack either automatically or by a Commander manually adding ("pulling") them into the stack. In the default configuration, a Candidate joins only when *manually* pulled by a Commander. You can reconfigure a Commander to *automatically* pull in Candidates that are in the default stacking configuration. You can also reconfigure a Candidate switch to either "push" itself into a particular Commander's stack, convert the Candidate to a Commander (for a stack that does not already have a Commander), or to operate as a standalone switch without stacking. The following table shows your control options for adding Members to a stack.

**Table 9-3. Stacking Configuration Guide**

| **Join Method**[1] | **Commander (IP Addressing Required)** | **Candidate (IP Addressing Optional)** | |
|---|---|---|---|
| | **Auto Grab** | **Auto Join** | **Passwords** |
| Automatically add Candidate to Stack (Causes the first 15 eligible, discovered switches in the subnet to automatically join a stack.) | **Yes** | **Yes** *(default)* | No *(default)*[*] |
| Manually add Candidate to Stack (Prevent automatic joining of switches you don't want in the stack) | **No** *(default)* | **Yes** *(default)* | Optional[*] |
| | **Yes** | **No** | Optional[*] |
| | **Yes** | **Yes** *(default)* or **No** | Configured |
| Prevent a switch from being a Candidate | N/A | **Disabled** | Optional |

[*]The Commander's Manager and Operator passwords propagate to the candidate when it joins the stack.



The easiest way to *automatically* create a stack is to:

1. Configure a switch as a Commander.
2. Configure IP addressing and a stack name on the Commander.
3. Set the Commander's **Auto Grab** parameter to **Yes**.
4. Connect Candidate switches (in their factory default configuration) to the network.

This approach automatically creates a stack of up to 16 switches (including the Commander). However this replaces manual control with an automatic process that may bring switches into the stack that you did not intend to include. With the Commander's **Auto Grab** parameter set to **Yes**, *any switch* conforming to all four of the following factors automatically becomes a stack Member:

- Default stacking configuration (**Stack State** set to **Candidate**, and **Auto Join** set to **Yes**)
- Same subnet (broadcast domain) and default VLAN as the Commander (If VLANs are used in the stack environment, see "Stacking Operation with a Tagged VLAN" on page 9-45.)
- No Manager password
- 14 or fewer stack members at the moment

### General Steps for Creating a Stack

This section describes the general stack creation process. For the detailed configuration processes, see pages 9-12 through 9-36 for the menu interface and pages 9-29 through 9-41 for the CLI.

1. Determine the naming conventions for the stack. You will need a stack name. Also, to help distinguish one switch from another in the stack, you can configure a unique system name for each switch. Otherwise, the system name for a switch appearing in the Stacking Status screen appears as the stack name plus an automatically assigned switch number. For example:

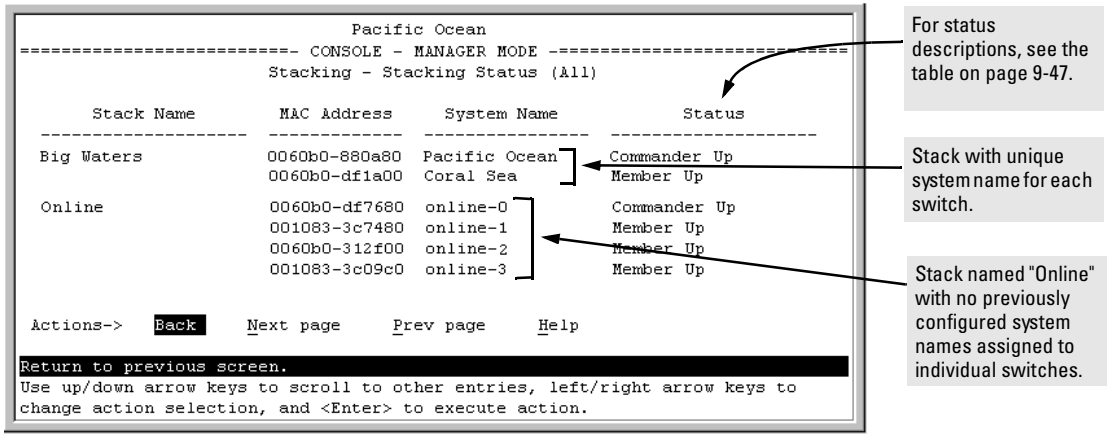



**Figure 9-4. Use of System Name to Help Identify Individual Switches**

2. Configure the Commander switch. Doing this first helps to establish consistency in your stack configuration, which can help prevent startup problems.

   - A stack requires one Commander switch. If you plan to implement more than one stack in a subnet (broadcast domain), the easiest way to avoid unintentionally adding a Candidate to the wrong stack is to manually control the joining process by leaving the Commander's **Auto Grab** parameter set to **No** (the default).
   - The Commander assigns its Manager and Operator passwords to any Candidate switch that joins the stack.
   - SNMP community names used in the Commander apply to stack members.

3. For automatically or manually pulling Candidate switches into a stack, you can leave such switches in their default stacking configuration. If you need to access Candidate switches through your network before they join the stack, assign IP addresses to these devices. Otherwise, IP addressing is optional for Candidates and Members. (Note that once a Candidate becomes a member, you can access it through the Commander to assign IP addressing or make other configuration changes.)
4. Make a record of any Manager passwords assigned to the switches (intended for your stack) that are not currently members. (You will have to use these passwords to enable the protected switches to join the stack.)
5. If you are using VLANs in the stacking environment, you must use the default VLAN for stacking links. For more information, see "Stacking Operation with a Tagged VLAN" on page 9-45.
6. Ensure that all switches intended for the stack are connected to the same subnet (broadcast domain). As soon as you connect the Commander, it will begin discovering the available Candidates in the subnet.
   - If you configured the Commander to automatically add Members (**Auto Grab** set to **Yes**), then the first 15 discovered Candidates meeting both of the following criteria will automatically become stack Members:
     - **Auto Join** parameter set to **Yes** (the default)
     - Manager password not configured
   - If you configured the Commander to manually add Members (**Auto Grab** set to **No**—the default), you can begin the process of selecting and adding the desired Candidates.
7. Ensure that all switches intended for the stack have joined.
8. If you need to perform specific configuration or monitoring tasks on a Member, use the console interface on the Commander to select and access the Member.

# Using the Menu Interface To View Stack Status And Configure Stacking

## Using the Menu Interface To View and Configure a Commander Switch

1. Configure an IP address and subnet mask on the Commander switch. (See "IP Configuration" on page 5-2.)
2. Display the Stacking Menu by selecting **Stacking** in the Main Menu.

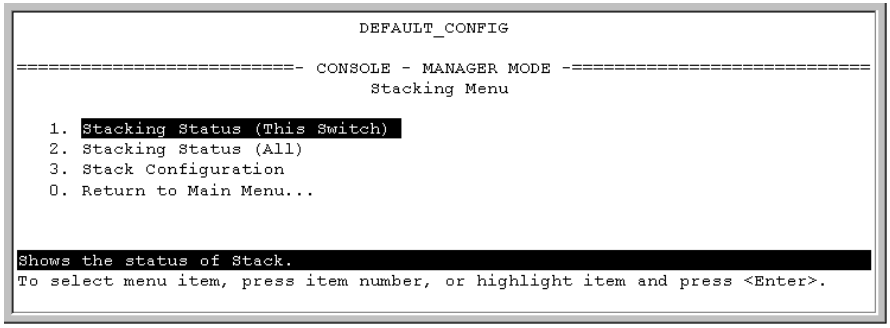



**Figure 9-5. The Default Stacking Menu**

3. Display the Stack Configuration menu by pressing to select **Stack Configuration**.

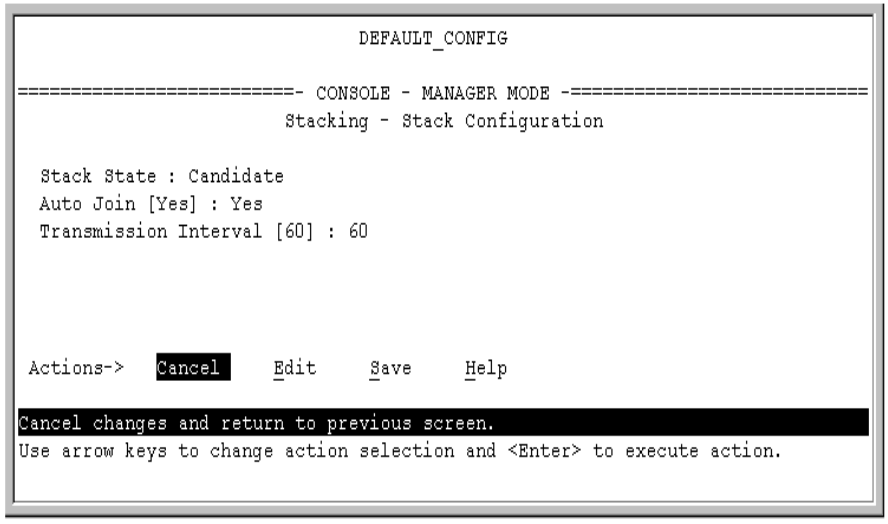



**Figure 9-6. The Default Stack Configuration Screen**

4. Move the cursor to the Stack State field by pressing [E] (for **Edit**). Then use the Space bar to select the **Commander** option.
5. Press the downarrow key to display the Commander configuration fields in the Stack Configuration screen.

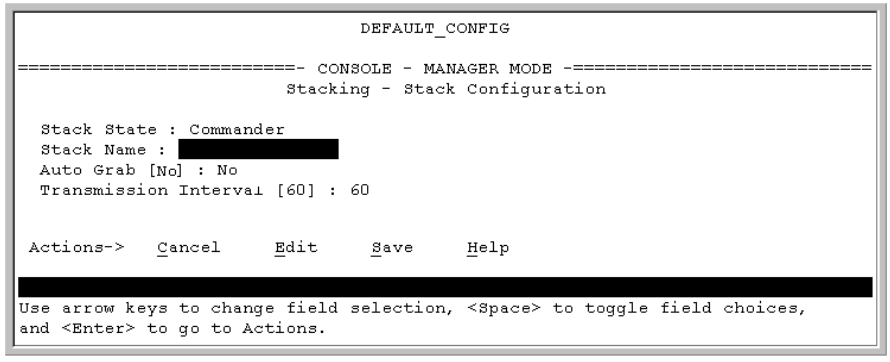



**Figure 9-7. The Default Commander Configuration in the Stack Configuration Screen**

6. Enter a unique stack name (up to 15 characters; no spaces) and press the downarrow key.
7. Ensure that the Commander has the desired **Auto Grab** setting, then press the downarrow key:

- **No** (the default) prevents automatic joining of Candidates that have their **Auto Join** set to **Yes**.
- **Yes** enables the Commander to automatically take a Candidate into the stack as a Member if the Candidate has **Auto Join** set to **Yes** (the default Candidate setting) and does not have a previously configured password.

8. Accept or change the transmission interval (default: 60 seconds), then press [Enter] to return the cursor to the **Actions** line.
9. Press [S] (for **Save**) to save your configuration changes and return to the Stacking menu.

Your Commander switch should now be ready to automatically or manually acquire Member switches from the list of discovered Candidates, depending on your configuration choices.

## Using the Menu To Manage a Candidate Switch

Using the menu interface, you can perform these actions on a Candidate switch:

- Add ("push") the Candidate into an existing stack
- Modify the Candidate's stacking configuration (**Auto Join** and **Transmission Interval**)
- Convert the Candidate to a Commander
- Disable stacking on the Candidate so that it operates as a standalone switch

In its default stacking configuration, a Candidate switch can either automatically join a stack or be manually added ("pulled") into a stack by a Commander, depending on the Commander's **Auto Grab** setting. The following table lists the Candidate's configuration options:

**Table 9-4.Candidate Configuration Options in the Menu Interface**

| Parameter | Default Setting | Other Settings |
|---|---|---|
| **Stack State** | Candidate | Commander, Member, or Disabled |
| **Auto Join** | Yes | No |
| **Transmission Interval** | 60 Seconds | Range: 1 to 300 seconds |



**Using the Menu To "Push" a Switch Into a Stack, Modify the Switch's Configuration, or Disable Stacking on the Switch.** Use Telnet or the web browser interface to access the Candidate if it has an IP address. Otherwise, use a direct connection from a terminal device to the switch's console port. (For information on how to use the web browser interface, see the online Help provided for the browser.)

1. Display the Stacking Menu by selecting **Stacking** in the console Main Menu.
2. Display the Stack Configuration menu by pressing [3] to select **Stack Configuration**.

```
                              DEFAULT_CONFIG

============================- CONSOLE - MANAGER MODE -=============================
                          Stacking - Stack Configuration

  Stack State : Candidate
  Auto Join [Yes] : Yes
  Transmission Interval [60] : 60




 Actions->   Cancel      Edit      Save      Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 9-8. The Default Stack Configuration Screen**

3. Move the cursor to the Stack State field by pressing [E] (for **Edit**).

4. Do one of the following:
   - To disable stacking on the Candidate, use the Space bar to select the **Disabled** option, then go to step 5.

     **Note:** Using the menu interface to disable stacking on a Candidate removes the Candidate from all stacking menus.
   - To insert the Candidate into a specific Commander's stack:
     i. Use the space bar to select Member.
     ii. Press [Tab] once to display the **Commander MAC Address** parameter, then enter the MAC address of the desired Commander.
   - To change **Auto Join** or **Transmission Interval**, use [Tab] to select the desired parameter, and:
     – To change **Auto Join**, use the Space bar.
     – To change **Transmission Interval**, type in the new value in the range of 1 to 300 seconds.

       **Note:** All switches in the stack must be set to the same transmission interval to help ensure proper stacking operation. SMC recommends that you leave this parameter set to the default 60 seconds.

   Then go to step 5.
5. press [Enter] to return the cursor to the **Actions** line.
6. Press [S] (for **Save**) to save your configuration changes and return to the Stacking menu.

## Using the Commander To Manage The Stack

The Commander normally operates as your stack manager and point of entry into other switches in the stack. This typically includes:

- Adding new stack members
- Moving members between stacks
- Removing members from a stack
- Accessing stack members for individual configuration changes and traffic monitoring

The Commander also imposes its passwords on all stack members and provides SNMP community membership to the stack. (See "SNMP Community Operation in a Stack" on page 9-44.)

**Using the Commander's Menu To Manually Add a Candidate to a Stack.** In the default configuration, you must manually add stack Members from the Candidate pool. Reasons for a switch remaining a Candidate instead of becoming a Member include any of the following:

- **Auto Grab** in the Commander is set to **No** (the default).
- **Auto Join** in the Candidate is set to **No**.

  **Note:** When a switch leaves a stack and returns to Candidate status, its **Auto Join** parameter resets to **No** so that it will not immediately rejoin a stack from which it has just departed.
- A Manager password is set in the Candidate.
- The stack is full.

Unless the stack is already full, you can use the Stack Management screen to manually convert a Candidate to a Member. If the Candidate has a Manager password, you will need to use it to make the Candidate a Member of the stack.

1. To add a Member, start at the Main Menu and select:

   **9. Stacking...**

   **4. Stack Management**

   You will then see the Stack Management screen:

```
                              Pacific Ocean

============================- CONSOLE - MANAGER MODE -==============================
                           Stacking - Stack Management

  SN   MAC Address     System Name     Device Type           Status
  --   -------------   -------------   -----------   -------------------------
  1    0060b0-df1a00   Coral Sea       SMC 10/100    Member Up
  2    080009-8c5080   North Atlantic  SMC 10/100    Member Up


  Actions->   Back     Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

For status descriptions, see the table on page 9-47.

**Figure 9-9. Example of the Stack Management Screen**

2. Press [A] (for **Add**) to add a Candidate. You will then see this screen listing the available Candidates:

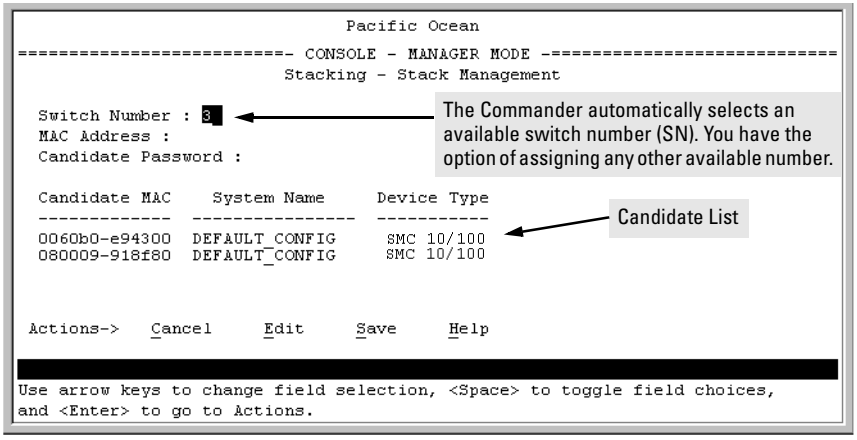



**Figure 9-10. Example of Candidate List in Stack Management Screen**

3. Either accept the displayed switch number or enter another available number. (The range is 0 - 15, with 0 reserved for the Commander.)

4. Use the downarrow key to move the cursor to the MAC Address field, then type the MAC address of the desired Candidate from the Candidate list in the lower part of the screen.

5. Do one of the following:

   - If the desired Candidate has a Manager password, press the downarrow key to move the cursor to the Candidate Password field, then type the password.
   - If the desired Candidate does not have a password, go to step 6.

6. Press [Enter] to return to the Actions line, then press [S] (for **Save**) to complete the Add process for the selected Candidate. You will then see a screen similar to the one in figure 9-11, below, with the newly added Member listed.

   **Note:** If the message **Unable to add stack member: Invalid Password** appears in the console menu's Help line, then you either omitted the Candidate's Manager password or incorrectly entered the Manager password.

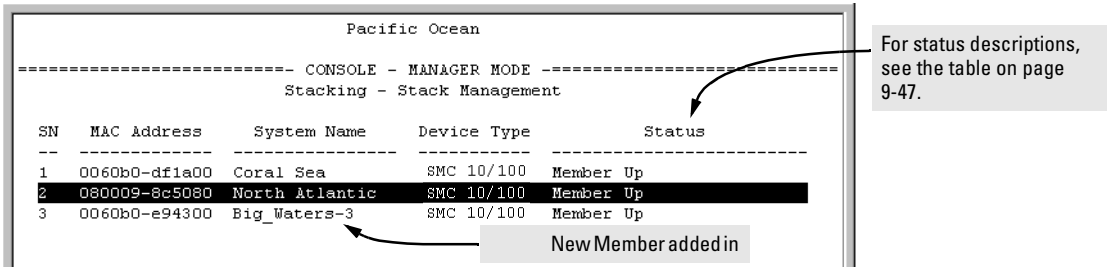



**Figure 9-11. Example of Stack Management Screen After New Member Added**

**Using the Commander's Menu To Move a Member From One Stack to Another.** Where two or more stacks exist in the same subnet (broadcast domain), you can easily move a Member of one stack to another stack if the destination stack is not full. (If you are using VLANs in your stack environment, see "Stacking Operation with a Tagged VLAN" on page 9-45.) This procedure is nearly identical to manually adding a Candidate to a stack (page 9-17). (If the stack from which you want to move the Member has a Manager password, you will need to know the password to make the move.)

1. To move a Member from one stack to another, go to the Main Menu of the Commander in the destination stack and display the Stacking Menu by selecting

   **9. Stacking...**

2. To learn or verify the MAC address of the Member you want to move, display a listing of all Commanders, Members, and Candidates in the subnet by selecting:

   **2. Stacking Status (All)**

   You will then see the Stacking Status (All) screen:

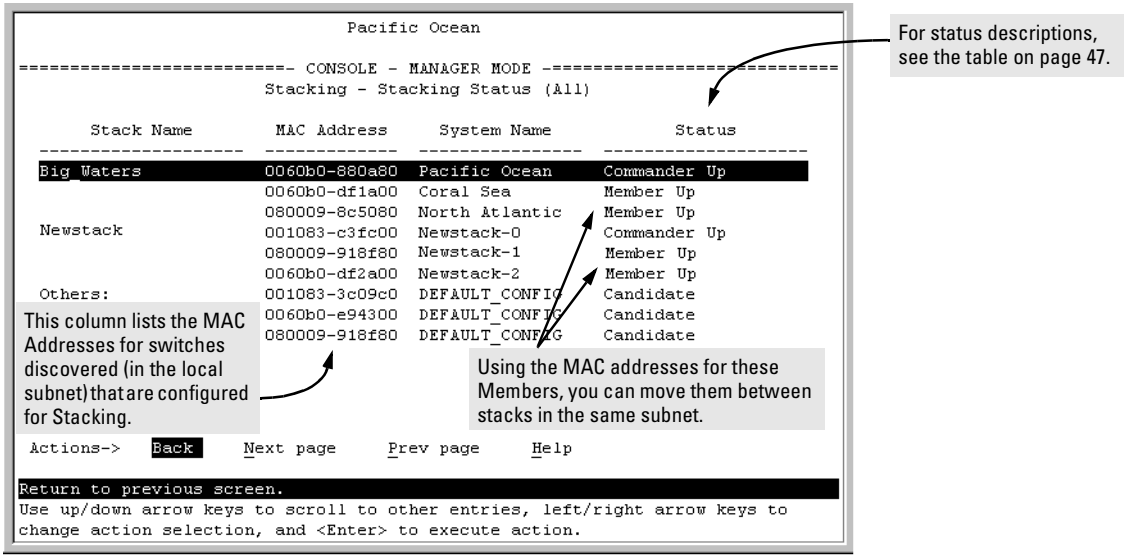



**Figure 9-12. Example of How the Stacking Status (All) Screen Helps You Find Member MAC Addresses**

3. In the Stacking Status (All) screen, find the Member switch that you want to move and note its MAC address, then press [B] (for **Back**) to return to the Stacking Menu.

4. Display the Commander's Stack Management screen by selecting

   **4. Stack Management**

   (For an example of this screen, see figure 9-9 on page 9-17.)

5. Press [A] (for **Add**) to add the Member. You will then see a screen listing any available candidates. (See figure 9-10 on page 9-18.) Note that you will not see the switch you want to add because it is a Member of another stack and not a Candidate.)

6. Either accept the displayed switch number or enter another available number. (The range is 0 - 15, with 0 reserved for the Commander.)

7. Use the downarrow key to move the cursor to the MAC Address field, then type the MAC address of the desired Member you want to move from another stack.

8. Do one of the following:
   - If the stack containing the Member you are moving has a Manager password, press the downarrow key to select the Candidate Password field, then type the password.
   - If the stack containing the Member you want to move does not have a password, go to step 9.
9. Press [Enter] to return to the Actions line, then press [S] (for **Save**) to complete the Add process for the selected Member. You will then see a screen similar to the one in figure 9-9 on page 9-17, with the newly added Member listed.

**Note:**

If the message **Unable to add stack member: Invalid Password** appears in the console menu's Help line, then you either omitted the Manager password for the stack containing the Member or incorrectly entered the Manager password.

You can "push" a Member from one stack to another by going to the Member's interface and entering the MAC address of the destination stack Commander in the Member's **Commander MAC Address** field. Using this method moves the Member to another stack without a need for knowing the Manager password in that stack, but also blocks access to the Member from the original Commander.

**Using the Commander's Menu To Remove a Stack Member.** These rules affect removals from a stack:

- When a Candidate becomes a Member, its **Auto Join** parameter is automatically set to **No**. This prevents the switch from automatically rejoining a stack as soon as you remove it from the stack.
- When you use the Commander to remove a switch from a stack, the switch rejoins the Candidate pool for your IP subnet (broadcast domain), with **Auto Join** set to **No**.
- When you remove a Member from a stack, it frees the previously assigned switch number (**SN**), which then becomes available for assignment to another switch that you may subsequently add to the stack. The default switch number used for an add is the lowest unassigned number in the Member range (1 - 15; 0 is reserved for the Commander).

To remove a Member from a stack, use the Stack Management screen.

1. From the Main Menu, select:

   **9. Stacking...**

#### 4. Stack Management

You will then see the Stack Management screen:

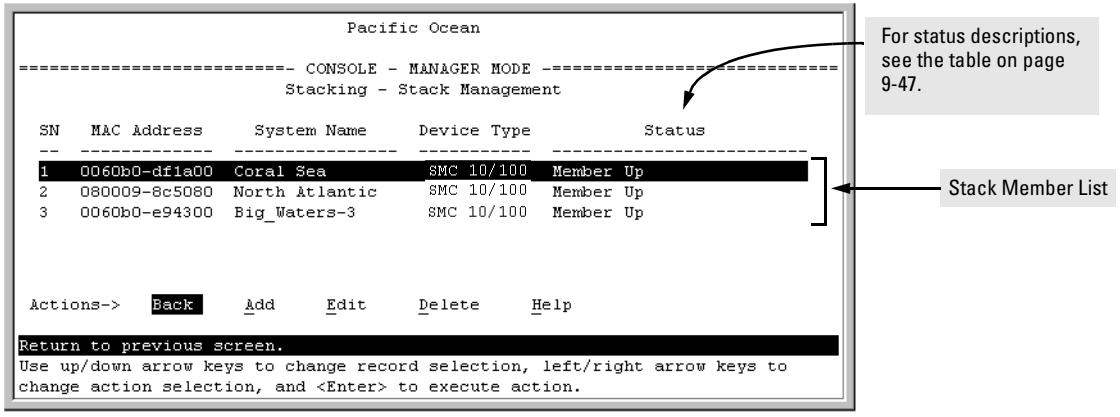



**Figure 9-13. Example of Stack Management Screen with Stack Members Listed**

2. Use the downarrow key to select the Member you want to remove from the stack.

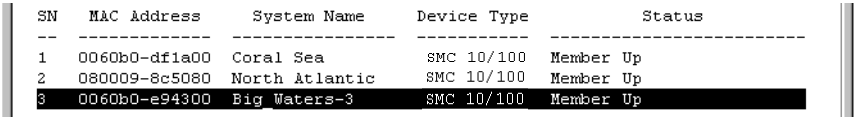



**Figure 9-14. Example of Selecting a Member for Removal from the Stack**

3. Type [D] (for **Delete**) to remove the selected Member from the stack. You will then see the following prompt:

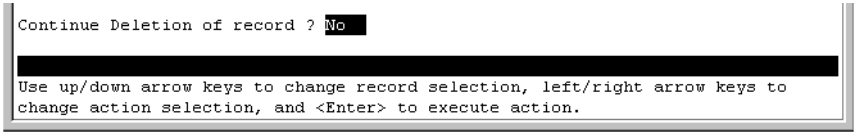



**Figure 9-15. The Prompt for Completing the Deletion of a Member from the Stack**

4. To continue deleting the selected Member, press the Space bar once to select **Yes** for the prompt, then press [Enter] to complete the deletion. The Stack Management screen updates to show the new stack Member list.

## Using the Commander To Access Member Switches for Configuration Changes and Monitoring Traffic

After a Candidate becomes a stack Member, you can use that stack's Commander to access the Member's console interface for the same configuration and monitoring that you would do through a Telnet or direct-connect access.

1. From the Main Menu, select:

   **9. Stacking...**
   **5. Stack Access**

   You will then see the Stack Access screen:

```
                              Pacific Ocean
==========================- CONSOLE - MANAGER MODE -==============================
                              Stacking - Stack Access

  SN   MAC Address     System Name      Device Type          Status
  --   -------------  ----------------  -----------  -------------------------
  0    0060b0-880a80  Pacific Ocean     SMC 10/100   Commander Up
  1    0060b0-df1a00  Coral Sea         SMC 10/100   Member Up
  2    080009-8c5080  North Atlantic    SMC 10/100   Member Up

 Actions->   Cancel     eXecute     Help

Return to previous screen.
Use arrow keys to change field selection
```

For status descriptions, see the table on page page 9-47.

**Figure 9-16. Example of the Stack Access Screen**

Use the downarrow key to select the stack Member you want to access, then press [X] (for **eXecute**) to display the console interface for the selected Member. For example, if you selected switch number 1 (system name: **Coral Sea**) in figure 9-16 and then pressed [X], you would see the Main Menu for the switch named Coral Sea.

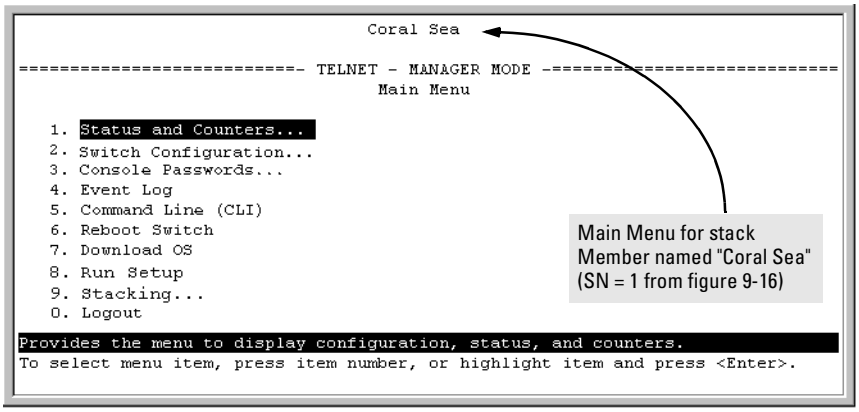



**Figure 9-17. The eXecute Command Displays the Console Main Menu for the Selected Stack Member**

2. You can now make configuration changes and/or view status data for the selected Member in the same way that you would if you were directly connected or telnetted into the switch.

3. When you are finished accessing the selected Member, do the following to return to the Commander's Stack Access screen:

   a. Return to the Member's Main Menu.

   b. Press [0] (for Logout), then [Y] (for Yes).

   c. Press [Return].

   You should now see the Commander's Stack Access screen. (For an example, see figure 9-16 on page 9-23.)

## Converting a Commander or Member to a Member of Another Stack

When moving a commander, the following procedure returns the stack members to Candidate status (with Auto-Join set to "**No**") and converts the stack Commander to a Member of another stack. When moving a member, the procedure simply pulls a Member out of one stack and pushes it into another.

1. From the Main Menu of the switch you want to move, select

   **9. Stacking**

2. To determine the MAC address of the destination Commander, select

   **2. Stacking Status (All)**

3. Press [B] (for **Back**) to return to the Stacking Menu.
4. To display Stack Configuration menu for the switch you are moving, select

   **3. Stack Configuration**

5. Press [E] (for **Edit**) to select the Stack State parameter.
6. Use the Space bar to select **Member**, then press [↓] to move to the **Commander MAC Address** field.
7. Enter the MAC address of the destination Commander and press [Enter].
8. Press [S] (for **Save**).



## Monitoring Stack Status

Using the stacking options in the menu interface for any switch in a stack, you can view stacking data for that switch or for all stacks in the subnet (broadcast domain). (If you are using VLANs in your stack environment, see "Stacking Operation with a Tagged VLAN" on page 9-45.) This can help you in such ways as determining the stacking configuration for individual switches, identifying stack Members and Candidates, and determining the status of individual switches in a stack. See table 9-5 on page 9-25.

**Table 9-5. Stack Status Environments**

| Screen Name | Commander | Member | Candidate |
|---|---|---|---|
| Stack Status (This Switch) | • Commander's stacking configuration<br>• Data on stack Members:<br>– Switch Number<br>– MAC Address<br>– System Name<br>– Device Type<br>– Status | • Member's stacking configuration<br>• Member Status<br>• Data identifying Member's Commander:<br>– Commander Status<br>– Commander IP Address<br>– Commander MAC Address | Candidate's stacking configuration |
| Stack Status (All) | Lists devices by stack name or Candidate status (if device is not a stack Member). Includes:<br>• Stack Name<br>• MAC Address<br>• System Name<br>• Status | Same as for Commander. | Same as for Commander. |

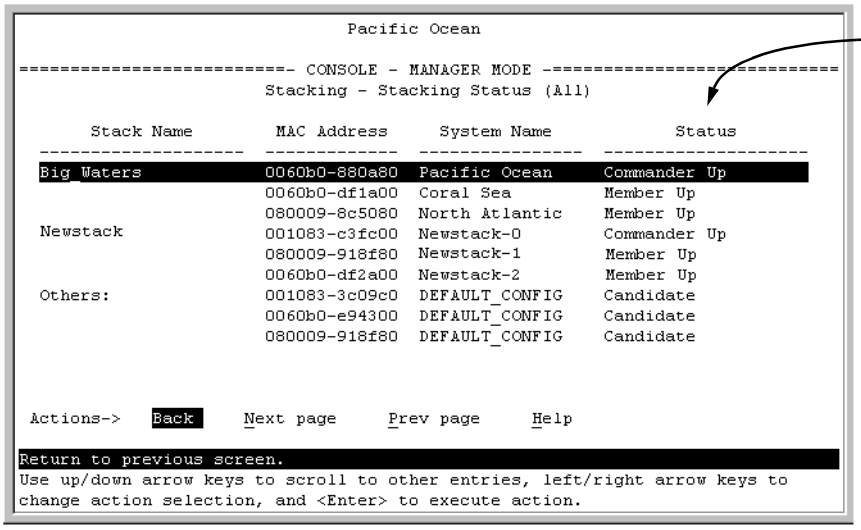
**Using Any Stacked Switch To View the Status for All Switches with Stacking Enabled.** This procedure displays the general status of all switches in the IP subnet (broadcast domain) that have stacking enabled.

1. Go to the console Main Menu for any switch configured for stacking and select:

   **9. Stacking ...**

   **2. Stacking Status (All)**

   You will then see a Stacking Status screen similar to the following:




For status descriptions, see the table on page 9-47.

**Figure 9-18. Example of Stacking Status for All Detected Switches Configured for Stacking**

**Viewing Commander Status.** This procedure displays the Commander and stack configuration, plus information identifying each stack member.

To display the status for a Commander, go to the console Main Menu for the switch and select:

**9. Stacking ...**

**1. Stacking Status (This Switch)**

You will then see the Commander's Stacking Status screen:

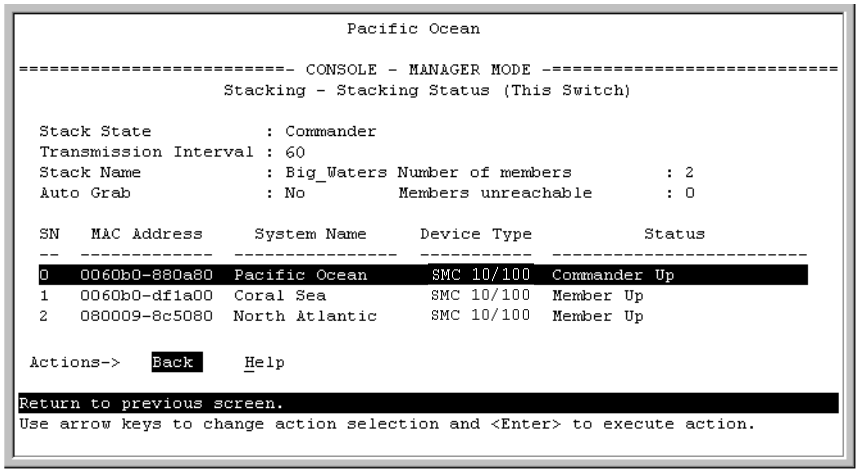



**Figure 9-19. Example of the Commander's Stacking Status Screen**

**Viewing Member Status.** This procedure displays the Member's stacking information plus the Commander's status, IP address, and MAC address.

To display the status for a Member:

1. Go to the console Main Menu of the Commander switch and select

   **9. Stacking ...**

   **5. Stack Access**

2. Use the downarrow key to select the Member switch whose status you want to view, then press [X] (for **eXecute**). You will then see the Main Menu for the selected Member switch.

3. In the Member's Main Menu screen, select

   **9. Stacking ...**

   **1. Stacking Status (This Switch)**

   You will then see the Member's Stacking Status screen:

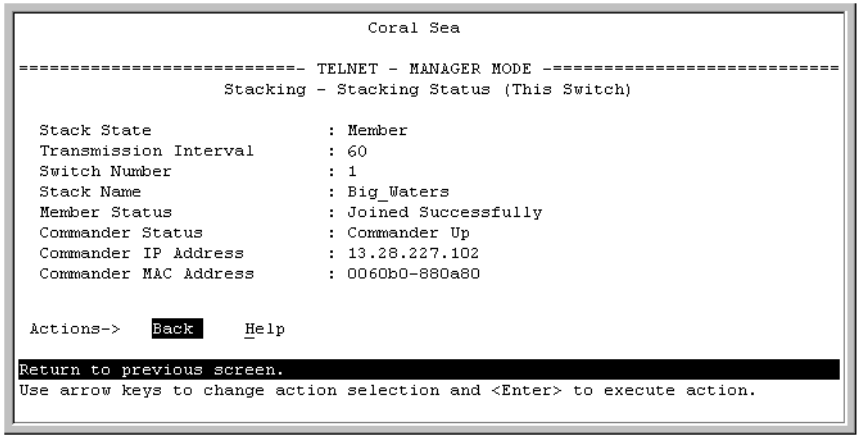



**Figure 9-20. Example of a Member's Stacking Status Screen**

**Viewing Candidate Status.** This procedure displays the Candidate's stacking configuration.

To display the status for a Candidate:

1. Use Telnet (if the Candidate has a valid IP address for your network) or a direct serial port connection to access the menu interface Main Menu for the Candidate switch and select

   **9. Stacking ...**

   **1. Stacking Status (This Switch)**

   You will then see the Candidate's Stacking Status screen:

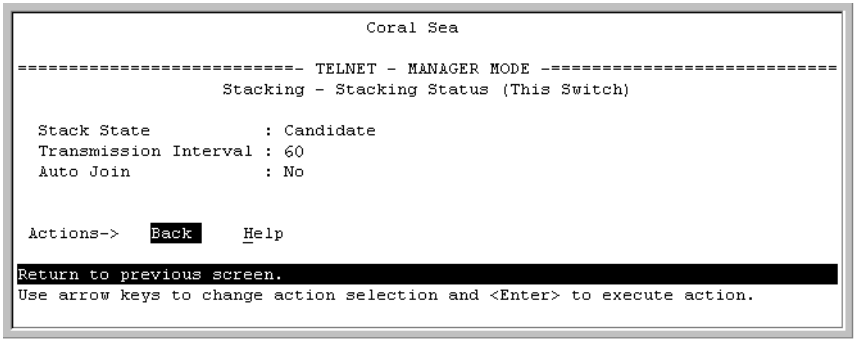



**Figure 9-21. Example of a Candidate's Stacking Screen**

# Using the CLI To View Stack Status and Configure Stacking

The CLI enables you to do all of the stacking tasks available through the menu interface.)

**Table 9-6. CLI Commands for Configuring Stacking on a Switch**

| CLI Command | Operation |
|---|---|
| **show stack [candidates \| view \| all]** | **Commander:** Shows Commander's stacking configuration and lists the stack members and their individual status.<br>**Member:** Lists Member's stacking configuration and status, and the status and the IP address and subnet mask of the stack Commander.<br><br>Options:<br>**candidates:** (Commander only) Lists stack Candidates.<br>**view:** (Commander only) Lists current stack Members and their individual status.<br>**all:** Lists all stack Commanders, Members and Candidates, with their individual status. |
| **[no] stack** | **Any Stacking-Capable Switch:** Enables or disables stacking on the switch.<br><br>**Default:** Stacking Enabled |
| **[no] stack commander *<stack name>*** | **Candidate or Commander:** Converts a Candidate to a Commander or changes the stack name of an existing commander.<br>"**No**" form eliminates named stack and returns Commander and stack Members to Candidate status with **Auto Join** set to **No**.<br><br>"**No**" form prevents the switch from being discovered as a stacking-capable switch.<br><br>**Default:** Switch Configured as a Candidate |
| **[no] stack auto-grab** | **Commander:** Causes Commander to automatically add to its stack any discovered Candidate in the subnet that does not have a Manager password and has **Auto-Join** set to **Yes**.<br><br>**Default:** Disabled<br>**Note:** If the Commander's stack already has 15 members, the Candidate cannot join until an existing member leaves the stack. |

| CLI Command | Operation |
|---|---|
| **[no] stack member** *<switch-num>* **mac-address** *<mac-addr>* **[password** *<password-str>***]** | **Commander:** Adds a Candidate to stack membership. "No" form removes a Member from stack membership. To easily determine the MAC address of a Candidate, use the **show stack candidates** command. To determine the MAC address of a Member you want to remove, use the **show stack view** command.The password (*password-str*) is required only when adding a Candidate that has a Manager password. |
| **telnet** *<1..15>*<br><br>*Used In:* Commander Only | **Commander:** Uses the **SN** (switch number— assigned by the stack Commander) to access the console interface (menu interface or CLI) of a stack member. To view the list of **SN** assignments for a stack, execute the **show stack** command in the Commander's CLI. |
| **[no] stack join** *<mac-addr>* | **Candidate:** Causes the Candidate to join the stack whose Commander has the indicated MAC address. "No" form is used in a Member to remove it from the stack of the Commander having the specified address.<br>**Member:** "Pushes" the member to another stack whose Commander has the indicated MAC address. |
| **[no] stack auto-join** | **Candidate:** Enables Candidate to automatically join the stack of any Commander in the IP subnet that has **Auto Grab** enabled, or disables **Auto-Join** in the candidate.<br><br>**Default: Auto Join** enabled.<br><br>**Note:** If the Candidate has a Manager password or if the available stack(s) already have the maximum of 15 Members, the automatic join will not occur. |
| **stack transmission-interval** | **All Stack Members:** specifies the interval in seconds for transmitting stacking discovery packets.<br><br>**Default:** 60 seconds |

## Using the CLI To View Stack Status

You can list the stack status for an individual switch and for other switches that have been discovered in the same subnet.

***Syntax:*** show stack [candidates | view | all]

**Viewing the Status of an Individual Switch.** The following example illustrates how to use the CLI in an SMC6624M to display the stack status for that switch. In this case, the switch is in the default stacking configuration.

***Syntax:*** show stack

```
Big_Waters-0(config)# show stack

 Stacking - Stacking Status (This Switch)

  Stack State           : Commander
  Transmission Interval : 60
  Stack Name            : Big_Waters     Number of members         : 0
  Auto Grab             : No             Members unreachable       : 0

  SN MAC Address   System Name      Device Type Status
  -- ------------- ---------------- ----------- -------------------------
  0  0001e7-c04100 Big_Waters-0      SMC 10/100 Commander Up
```

**Figure 9-22. Example of Using the Show Stack Command To List the Stacking Configuration for an Individual Switch**

**Viewing the Status of Candidates the Commander Has Detected.**

This example illustrates how to list stack candidates the Commander has discovered in the ip subnet (broadcast domain).

Syntax: show stack candidates

```
Big_Waters-0(config)# show stack candidates
  Stack Candidates
   Candidate MAC System Name                Device Type
   ------------- ------------------------- -----------
   0060b0-889e00 DEFAULT_CONFIG             SMC 10/100
```

**Figure 9-23. Example of Using the Show Stack Candidates Command To List Candidates**

**Viewing the Status of all Stack-Enabled Switches Discovered in the IP Subnet.** The next example lists all the stack-configured switches discovered in the IP subnet. Because the SMC6624M on which the **show stack all** command was executed is a candidate, it is included in the "Others" category.

***Syntax:*** show stack all

```
Stacking - Stacking Status (All)

 Stack Name      MAC Address   System Name               Status
 --------------- ------------- ------------------------- -------------
 Big_Waters      0030c1-7fcc40 SMC 10/100                Commander Up
                 0030c1-7fec40 Big_Waters-1              Member Up
 Others:         0060b0-889e00 DEFAULT_CONFIG            Candidate
```

**Figure 9-24. Result of Using the Show Stack All Command To List Discovered Switches in the IP Subnet**

**Viewing the Status of the Commander and Current Members of the Commander's Stack.** The next example lists all switches in the stack of the selected switch.

***Syntax:*** show stack view

```
Stack Members
 SN MAC Address   System Name      Device Type Status
 -- ------------- ---------------- ----------- --------------
 0  0030c1-7fcc40 HP2512            SMC 10/100  Commander Up
 1  0030c1-7fec40 Big_Waters-1      SMC 10/100  Member Up
```

**Figure 9-25. Example of the Show Stack View Command To List the Stack Assigned to the Selected Commander**

## Using the CLI To Configure a Commander Switch

You can configure any stacking-enabled switch to be a Commander as long as the intended stack name does not already exist on the broadcast domain. (When you configure a Commander, you automatically create a corresponding stack.)

Before you begin configuring stacking parameters:

1. Configure IP addressing on the switch intended for stack commander and, if not already configured, on the primary VLAN. (For more on configuring IP addressing, see "IP Configuration" on page 5-2.)

**Note**

The primary VLAN must have an IP address in order for stacking to operate properly. For more on the primary VLAN, see "Which VLAN Is Primary?" on page 9-51.

2. Configure a Manager password on the switch intended for commander. (The Commander's Manager password controls access to stack Members.) For more on passwords, see chapter 7, "Using Passwords, Port Security, and Authorized Managers To Protect Against Unauthorized Access".

**Configure the Stack Commander.** Assigning a stack name to a switch makes it a Commander and automatically creates a stack.

***Syntax:*** stack commander *<name-str>*

This example creates a Commander switch with a stack name of **Big_Waters**. (Note that if stacking was previously disabled on the switch, this command also enables stacking.)

```
SMC TigerSwitch 10/100(config)# stack commander Big_Waters
```

As the following **show stack** display shows, the Commander switch is now ready to add members to the stack.

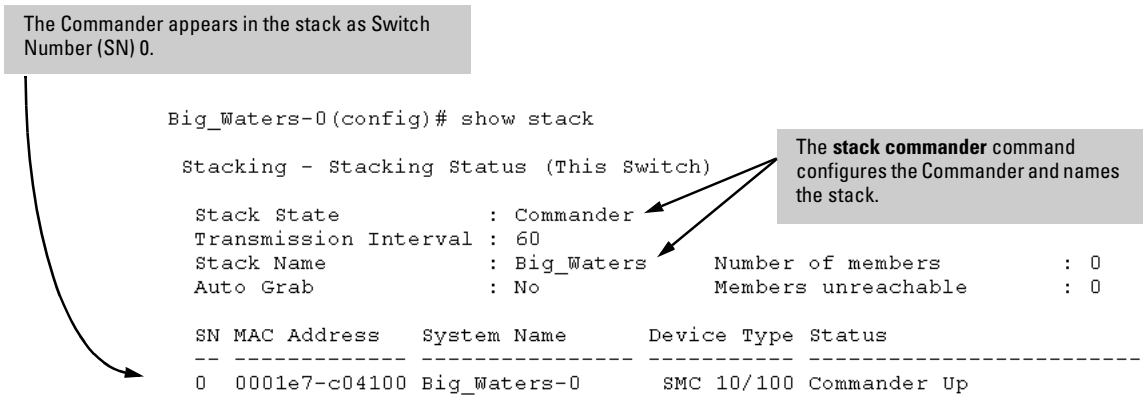



**Figure 9-26. Example of the Commander's Show Stack Screen with Only the Commander Discovered**

**Using a Member's CLI to Convert the Member to the Commander of a New Stack.** This procedure requires that you first remove the Member from its current stack, then create the new stack. If you do not know the MAC address for the Commander of the current stack, use **show stack** to list it.

***Syntax:*** no stack
stack commander *<stack name>*

Suppose, for example, that an SMC6624M named "Bering Sea" is a Member of a stack named "Big_Waters". To use the switch's CLI to convert it from a stack Member to the Commander of a new stack named "Lakes", you would use the following commands:

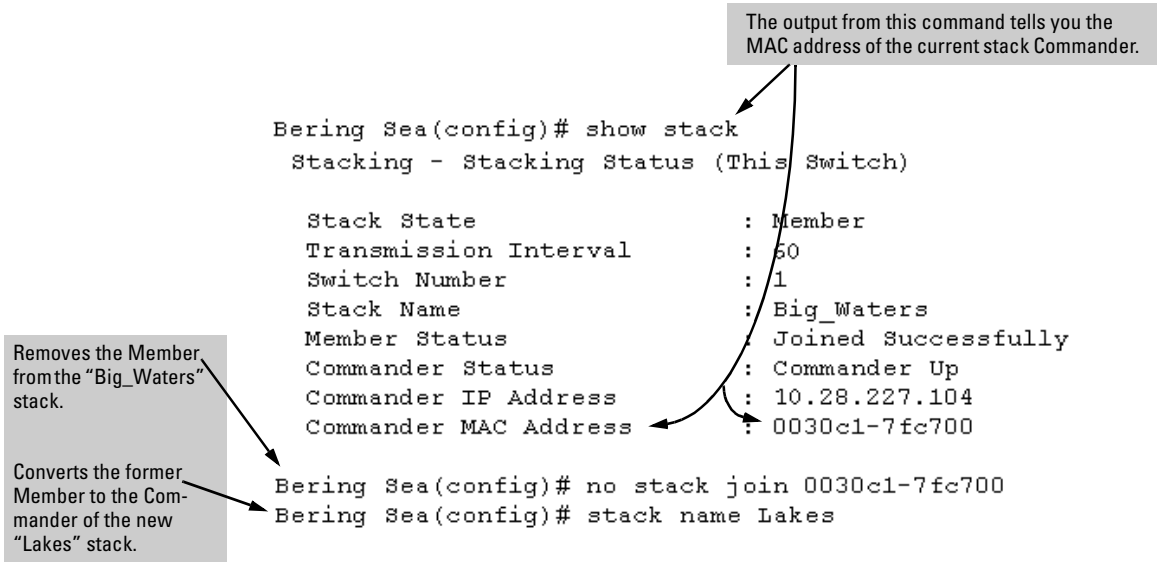



**Figure 9-27. Example of Using a Member's CLI To Convert the Member to the Commander of a New Stack**

## Adding to a Stack or Moving Switches Between Stacks

You can add switches to a stack by adding discovered Candidates or by moving switches from other stacks that may exist in the same subnet. (You cannot add a Candidate that the Commander has not discovered.)

In its default configuration, the Commander's **Auto-Grab** parameter is set to **No** to give you manual control over which switches join the stack and when they join. This prevents the Commander from automatically trying to add every Candidate it finds that has **Auto Join** set to **Yes** (the default for the Candidate).

(If you want any eligible Candidate to automatically join the stack when the Commander discovers it, configure **Auto Grab** in the Commander to **Yes**. When you do so, *any* Candidate discovered with **Auto Join** set to **Yes** (the default) and no Manager password will join the stack, up to the limit of 15 Members.)

**Using the Commander's CLI To Manually Add a Candidate to the Stack.** To manually add a candidate, you will use:

- A switch number (**SN**) to assign to the new member. Member SNs range from 1 to 15. To see which SNs are already assigned to Members, use **show stack view**. You can use any SN not included in the listing. (SNs are viewable only on a Commander switch.)
- The MAC address of the discovered Candidate you are adding to the stack. To see this data, use the **show stack candidates** listing .

For example:

```
Big_Waters-0(config)# show stack view
 Stack Members
  SN MAC Address    System Name       Device Type Status
  -- -------------- ----------------- ----------- --------------------------
  0  0030c1-7fec40 Big_Waters-0       SMC 10/100 Commander Up
  1  0060b0-880a80 Indian Ocean       SMC 10/100 Member Up
```

In this stack, the only SNs in use are 0 and 1, so you can use any SN number from 2 through 15 for new Members. (The SN of "0" is always reserved for the stack Commander.)

**Note:** When manually adding a switch, you must assign an SN. However, if the Commander automatically adds a new Member, it assigns an SN from the available pool of unused SNs.

**Figure 9-28. Example of How To Determine Available Switch Numbers (SNs)**

To display all discovered Candidates with their MAC addresses, execute **show stack candidates** from the Commander's CLI. For example, to list the discovered candidates for the above Commander:

```
Big_Waters-0(config)# show stack candidates
  Stack Candidates
   Candidate MAC System Name                Device Type
   ------------- -------------------------- -----------
   0030c1-b24ac0 North Sea                   SMC 10/100
   0060b0-df1a00 DEFAULT_CONFIG              SMC 10/100
```

MAC addresses of discovered Candidates.

**Figure 9-29. Example of How To Determine MAC Addresses of Discovered Candidates**

Knowing the available switch numbers (**SN**s) and Candidate MAC addresses, you can proceed to manually assign a Candidate to be a Member of the stack:

***Syntax:*** stack member <*switch-number*> mac-address <*mac-addr*> [password <*password-str*>]

For example, if the switch named "DEFAULT_CONFIG" in the above listing did not have a Manager password and you wanted to make it a stack Member with an **SN** of **2**, you would execute the following command:

```
SMC TigerSwitch 10/100(config)# stack member 2 mac-
address 0060b0-df1a00
```

The **show stack view** command then lists the Member added by the above command:

```
Big_Waters-0(config)# show stack view
 Stack Members
  SN MAC Address   System Name      Device Type Status
  -- ------------- ---------------- ----------- -------------------------
  0  0030c1-7fec40 Big_Waters-0      SMC 10/100 Commander Up
  1  0060b0-880a80 Indian Ocean      SMC 10/100 Member Up
  2  0060b0-df1a00 Big_Waters-2      SMC 10/100 Member Up
```

SN (Switch Number) 2 is the new Member added by the **stack member** command.

The new member did not have a System Name configured prior to joining the stack, and so receives a System Name composed of the stack name (assigned in the Commander) with its SN number as a suffix.

**Figure 9-30. Example Showing the Stack After Adding a New Member**

**Using Auto Join on a Candidate.** In the default configuration, a Candidate's Auto Join parameter is set to "Yes", meaning that it will automatically join a stack if the stack's Commander detects the Candidate and the Commander's Auto Grab parameter is set to "Yes". You can disable Auto Join on a Candidate if you want to prevent automatic joining in this case. There is also the instance where a Candidate's Auto Join is disabled, for example, when a Commander leaves a stack and its members automatically return to Candidate status, or if you manually remove a Member from a stack. In this case, you may want to reset Auto Join to "Yes".

***Status:*** [no] stack auto-join

```
SMC TigerSwitch 10/100(config)# no  stack auto-join
```
Disables Auto Join on a Candidate.

```
SMC TigerSwitch 10/100(config)# stack auto-join
```
Enables Auto Join on a Candidate.

**Using a Candidate CLI To Manually "Push" the Candidate Into a Stack .** Use this method if any of the following apply:

- The Candidate's **Auto Join** is set to **Yes** (and you do not want to enable **Auto Grab** on the Commander) or the Candidate's **Auto Join** is set to **No**.
- Either you know the MAC address of the Commander for the stack into which you want to insert the Candidate, or the Candidate has a valid IP address and is operating in your network.

***Syntax:*** stack join *<mac-addr>*

where: *<mac-addr>* is the MAC address of the Commander in the destination stack.

Use Telnet (if the Candidate has an IP address valid for your network) or a direct serial port connection to access the CLI for the Candidate switch. For example, suppose that a Candidate named "North Sea" with **Auto Join** off and a valid IP address of 10.2.13.104 is running on a network. You could Telnet to the Candidate, use **show stack all** to determine the Commander's MAC address, and then "push" the Candidate into the desired stack.

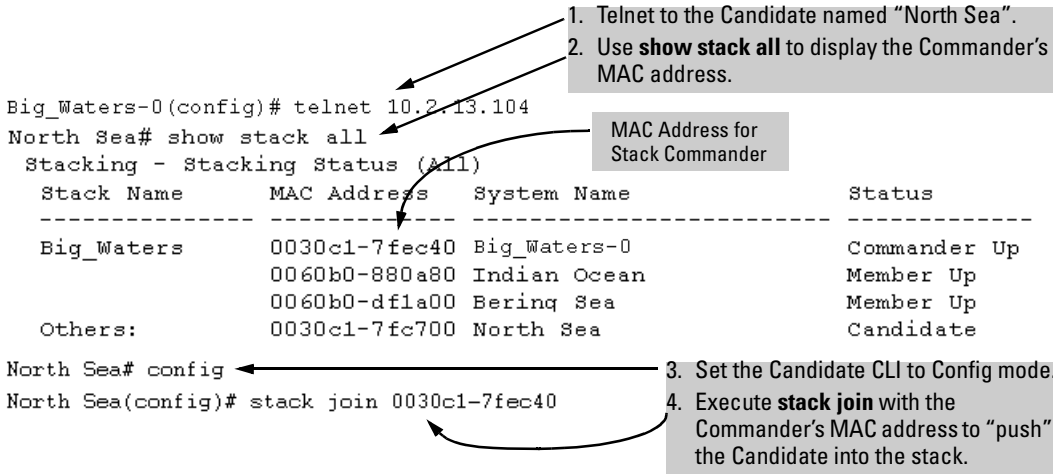



**Figure 9-31. Example of "Pushing" a Candidate Into a Stack**

To verify that the Candidate successfully joined the stack, execute **show stack all** again to view the stacking status.

**Using the Destination Commander CLI To "Pull" a Member from Another Stack.** This method uses the Commander in the destination stack to "pull" the Member from the source stack.

***Syntax:*** stack member <*switch-number*>
mac-address <*mac-addr*>
[password<*password-str*>]

In the destination Commander, use **show stack all** to find the MAC address of the Member you want to pull into the destination stack. For example, suppose you created a new Commander with a stack name of "Cold_Waters" and you wanted to move a switch named "Bering Sea" into the new stack:



```
Big_Waters-0(config)# show stack all
 Stacking - Stacking Status (All)
  Stack Name      MAC Address   System Name                Status
  --------------- ------------- -------------------------- -------------
  Big_Waters      0030c1-7fec40 Big_Waters-0               Commander Up
                  0060b0-880a80 Indian Ocean               Member Up
                  0060b0-df1a00 Bering Sea                 Member Up
  Cold_Waters     0030c1-7fc700 Cold_Waters-0              Commander Up
```

Move this switch into the "Cold Waters"

**Figure 9-32. Example of Stack Listing with Two Stacks in the Subnet**

You would then execute the following command to pull the desired switch into the new stack:

```
SMC TigerSwitch 10/100(config)# stack member 1 mac-
address 0060b0-df1a00
```

*Where* **1** is an unused switch number (**SN**).

Since a password is not set on the Candidate, a password is not needed in this example.

You could then use **show stack all** again to verify that the move took place.

**Using a Member CLI To "Push" the Member into Another Stack.** You can use the Member's CLI to "push" an SMC6624M stack Member into a destination stack if you know the MAC address of the destination Commander.

***Syntax:*** stack join <*mac-addr*>

*where:* <*mac-addr*> is the MAC address of the Commander for the destination stack.

**Converting a Commander to a Member of Another Stack.** Removing the Commander from a stack eliminates the stack and returns its Members to the Candidate pool with **Auto Join** disabled.

***Syntax:*** no stack name *<stack name>*
stack join *<mac-address>*

If you don't know the MAC address of the destination Commander, you can use **show stack all** to identify it.

For example, suppose you have a switch operating as the Commander for a temporary stack named "Test". When it is time to eliminate the temporary "Test" stack and convert the switch into a member of an existing stack named "Big_Waters", you would execute the following commands in the CLI of the switch:

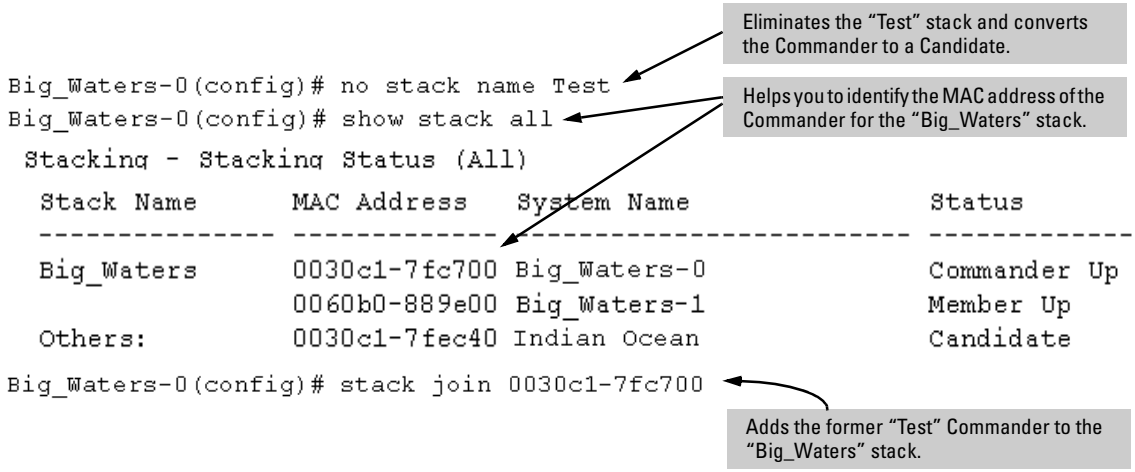



**Figure 9-33. Example of Command Sequence for Converting a Commander to a Member**

## Using the CLI To Remove a Member from a Stack

You can remove a Member from a stack using the CLI of either the Commander or the Member.

**Note**

When you remove a Member from a stack, the Member's **Auto Join** parameter is set to **No**.

**Using the Commander CLI To Remove a Stack Member.** This option requires the switch number (SN) and the MAC address of the switch to remove. (Because the Commander propagates its Manager password to all stack members, knowing the Manager password is necessary only for gaining access to the Commander.)

***Syntax:*** [no] stack member <*switch-num*> mac-address <*mac-addr*>

Use **show stack view** to list the stack Members. For example, suppose that you wanted to use the Commander to remove the "North Sea" Member from the following stack:

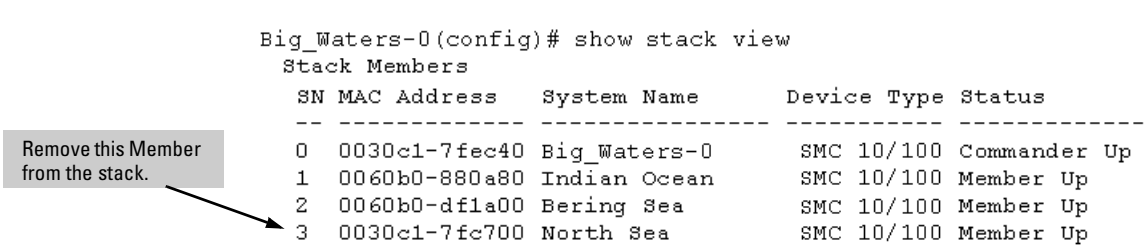



**Figure 9-34. Example of a Commander and Three Switches in a Stack**

You would then execute this command to remove the "North Sea" switch from the stack:

```
Big_Waters-0(config)# no stack member 3 mac-address 0030c1-
7fc700
```

*where:*

- **3** is the "North Sea" Member's switch number (**SN**)
- **0030c1-7fc700** is the "North Sea" Member's MAC address

**Using the Member's CLI To Remove the Member from a Stack.**

***Syntax:*** no stack join <*mac-addr*>

To use this method, you need the Commander's MAC address, which is available using the show stack command in the Member's CLI. For example:

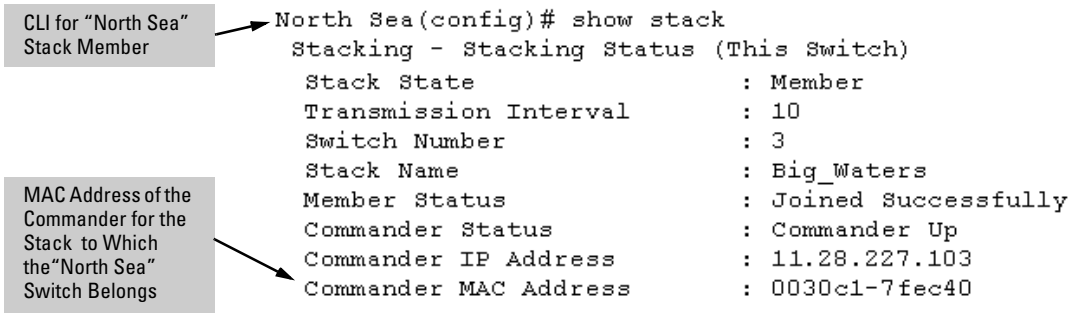



**Figure 9-35. Example of How To Identify the Commander's MAC Address from a Member Switch**

You would then execute this command in the "North Sea" switch's CLI to remove the switch from the stack:

```
North Sea(config)# no stack join 0030c1-7fec40
```

## Using the CLI To Access Member Switches for Configuration Changes and Traffic Monitoring

After a Candidate becomes a Member, you can use the telnet command from the Commander to access the Member's CLI or console interface for the same configuration and monitoring that you would do through a Telnet or direct-connect access from a terminal.

***Syntax:*** telnet *<switch-number>*

*where:* unsigned integer is the switch number (**SN**) assigned by the Commander to each member (range: **1** - **15**).

To find the switch number for the Member you want to access, execute the **show stack view** command in the Commander's CLI. For example, suppose that you wanted to configure a port trunk on the switch named "North Sea" in the stack named "Big_Waters". Do do so you would go to the CLI for the "Big_Waters" Commander and execute show stack view to find the switch number for the "North Sea" switch:

The switch number (**SN**) for the "North Sea" switch is "**3**".

```
Big_Waters-0(config)# show stack view
 Stack Members
  SN MAC Address   System Name       Device Type Status
  -- ------------- ----------------- ----------- -------------
  0  0030c1-7fec40 Big_Waters-0       SMC 10/100 Commander Up
  1  0060b0-880a80 Indian Ocean       SMC 10/100 Member Up
  2  0060b0-df1a00 Bering Sea         SMC 10/100 Member Up
  3  0030c1-7fc700 North Sea          SMC 10/100 Member Up
```

**Figure 9-36. Example of a Stack Showing Switch Number (SN) Assignments**

To access the "North Sea" console, you would then execute the following **telnet** command:

```
Big_Waters-0(config)# telnet 3
```

You would then see the CLI prompt for the "North Sea" switch, allowing you to configure or monitor the switch as if you were directly connected to the console.

## SNMP Community Operation in a Stack

### Community Membership

In the default stacking configuration, when a Candidate joins a stack, it automatically becomes a Member of any SNMP community to which the Commander belongs, even though any community names configured in the Commander are not propagated to the Member's SNMP Communities listing. However, if a Member has its own (optional) IP addressing, it can belong to SNMP communities to which other switches in the stack, including the Commander, do not belong. For example:

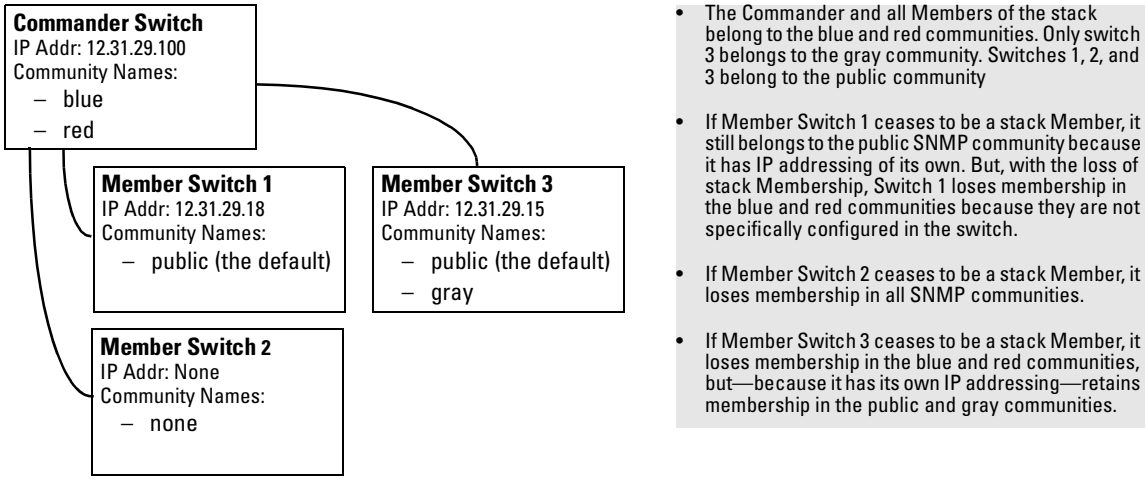



**Figure 9-37. Example of SNMP Community Operation with Stacking**

**SNMP Management Station Access to Members Via the Commander.**

To use a management station for SNMP Get or Set access through the Commander's IP address to a Member, you must append **@sw<switch number>** to the community name. For example, in figure 9-37, you would use the following command in your management station to access Switch 1's MIB using the blue community:

snmpget <*MIB variable*> 10.31.29.100 blue@sw1

Note that because the gray community is only on switch 3, you could not use the Commander IP address for gray community access from the management station. Instead, you would access switch 3 directly using the switch's own IP address. For example:

**snmpget <*MIB variable*> 10.31.29.15 gray**

Note that in the above example (figure 9-37) you cannot use the public community through the Commander to access any of the Member switches. For example, you can use the public community to access the MIB in switches 1 and 3 by using their unique IP addresses. However, you must use the red or blue community to access the MIB for switch 2.

**snmpget *<MIB variable>* 10.31.29.100 blue@sw2**



## Using the CLI To Disable or Re-Enable Stacking

In the default configuration, stacking is enabled on the SMC6624M. You can use the CLI to disable stacking on the switch at any time. Disabling stacking has the following effects:

- **Disabling a Commander:** Eliminates the stack, returns the stack Members to Candidates with **Auto Join** disabled, and changes the Commander to a stand-alone (nonstacking) switch. You must re-enable stacking on the switch before it can become a Candidate, Member, or Commander.
- **Disabling a Member:** Removes the Member from the stack and changes it to a stand-alone (nonstacking) switch. You must re-enable stacking on the switch before it can become a Candidate, Member, or Commander.
- **Disabling a Candidate:** Changes the Candidate to a stand-alone (nonstacking) switch.

***Syntax:*** no stack (Disables stacking on the switch.)
stack (Enables stacking on the switch.)

## Transmission Interval

All switches in the stack must be set to the same transmission interval to help ensure proper stacking operation. SMC recommends that you leave this parameter set to the default 60 seconds.

***Syntax:*** stack transmission-interval <*seconds*>

## Stacking Operation with Multiple VLANs Configured

Stacking uses the primary VLAN in a switch. In the factory-default configuration, the DEFAULT_VLAN is the primary VLAN. However, you can designate any VLAN configured in the switch as the primary VLAN. (See “Which VLAN Is Primary?” on page 9-51.)

When using stacking in a multiple-VLAN environment, the following criteria applies:

- Stacking uses only the primary VLAN on each switch in a stack.
- The primary VLAN can be tagged or untagged as needed in the stacking path from switch to switch.
- The same VLAN ID (VID) must be assigned to the primary VLAN in each stacked switch.

## Web: Viewing and Configuring Stacking

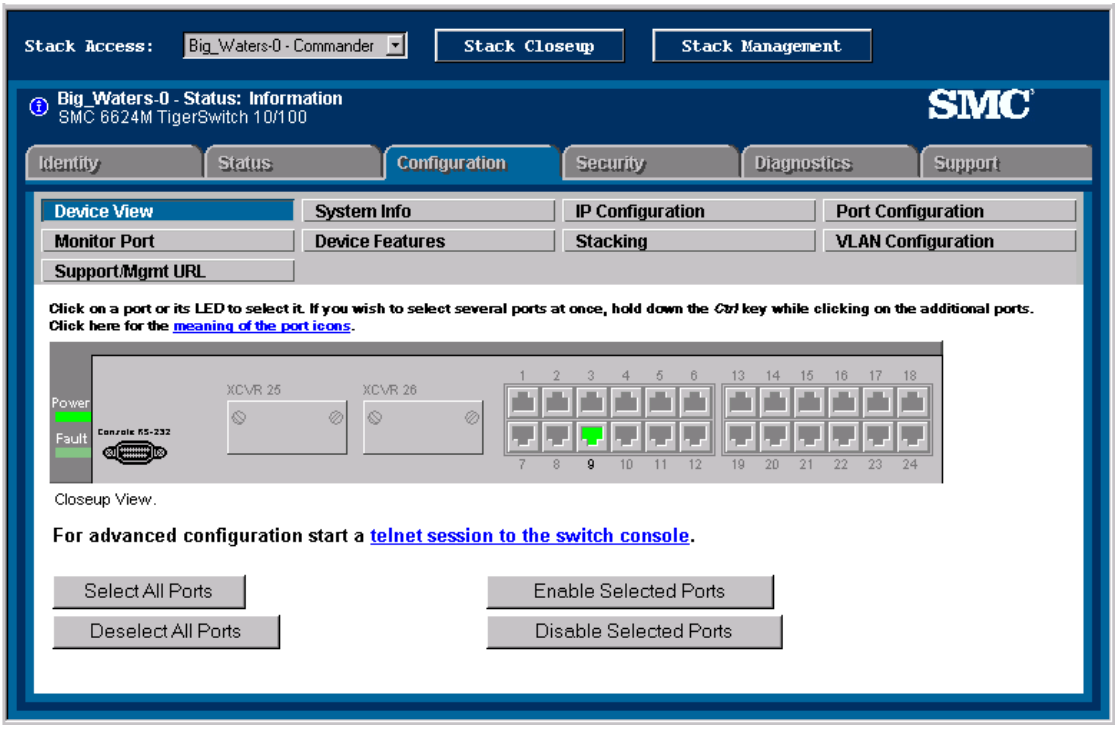



**Figure 9-38. Example of the Web Browser Interface for a Commander**

The web browser interface for a Commander appears as shown above. The interface for Members and Candidates appears the same as for a non-stacking SMC6624M switch.

To view or configure stacking on the web browser interface:

1. Click on the **Configuration** tab.
2. Click on [Stacking] to display the stackingconfiguration for an individual switch, and make any configuration changes you want for that switch.

3. Click on [Apply Changes] to save any configuration changes for the individual switch.
4. If the switch is a Commander, use the [Stack Closeup] and [Stack Management] buttons for viewing and using stack features.

## Status Messages

Stacking screens and listings display these status messages:

| Message | Condition | Action or Remedy |
|---|---|---|
| Candidate Auto-join | Indicates a switch configured with Stack State set to **Candidate, Auto Join** set to **Yes** (the default), and no Manager password. | None required |
| Candidate | Candidate cannot automatically join the stack because one or both of the following conditions apply:<br>• Candidate has **Auto Join** set to **No**.<br>• Candidate has a Manager password. | Manually add the candidate to the stack. |
| Commander Down | Member has lost connectivity to its Commander. | Check connectivity between the Commander and the Member. |
| Commander Up | The Member has stacking connectivity with the Commander. | None required. |
| Mismatch | This may be a temporary condition while a Candidate is trying to join a stack. If the Candidate does not join, then stack configuration is inconsistent. | Initially, wait for an update. If condition persists, reconfigure the Commander or the Member. |
| Member Down | A Member has become detached from the stack. A possible cause is an interruption to the link between the Member and the Commander. | Check the connectivity between the Commander and the Member. |
| Member Up | The Commander has stacking connectivity to the Member. | None required. |
| Rejected | The Candidate has failed to be added to the stack. | The candidate may have a password. In this case, manually add the candidate. Otherwise, the stack may already be full. A stack can hold up to 15 Members (plus the Commander). |

# Port-Based Virtual LANs (Static VLANs)

**VLAN Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view existing VLANs | n/a | page 9-55 thru 9-60 | page 9-61 | page 9-66 |
| configuring static VLANs | default VLAN with VID = 1 | page 9-55 thru 9-60 | page 9-60 | page 9-66 |
| configuring dynamic VLANs | disabled | See "GVRP" on page 9-74. | | |

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. (That is, all ports carrying traffic for a particular subnet address would normally belong to the same VLAN.)

**Note**

This section describes *static* VLANs, which are VLANs you manually configure with a name, VLAN ID (VID), and port assignments. (For information on *dynamic* VLANs, see "GVRP" on page 9-74.)

Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources.

By default, the SMC6624M switch is 802.1Q VLAN enabled and allows up to 30 port-based VLANs (default: 8). For information on GVRP, see "GVRP" on page 9-74. (The 802.1Q compatibility enables you to assign each switch port to multiple VLANs, if needed, and the port-based nature of the configuration allows interoperation with older switches that require a separate port for each VLAN.)

**General Use and Operation.** Port-based VLANs are typically used to enable broadcast traffic reduction and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on a switch. Packets are forwarded only between ports that are designated for the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is

saved by not allowing packets to flood out all ports. An external router is required to enable separate VLANs on a switch to communicate with each other.

For example, referring to figure 9-39, if ports 1 through 4 belong to VLAN_1 and ports 5 through 8 belong to VLAN_2, traffic from end-node stations on ports 2 through 4 is restricted to only VLAN_1, while traffic from ports 5 through 7 is restricted to only VLAN_2. For nodes on VLAN_1 to communicate with VLAN_2, their traffic must go through an external router via ports 1 and 8.

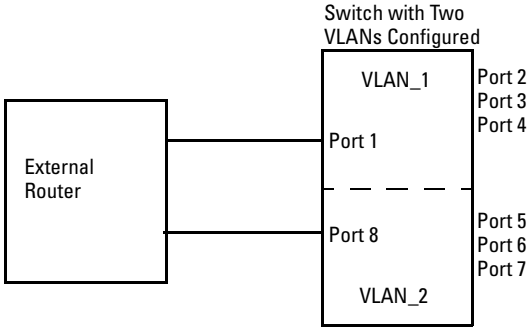



**Figure 9-39. Example of Routing Between VLANs via an External Router**

**Overlapping (Tagged) VLANs.** A port on the SMC6624M switch can be a member of more than one VLAN if the device to which it is connected complies with the 802.1Q VLAN standard. For example, a port connected to a central server using a network interface card (NIC) that complies with the 802.1Q standard can be a member of multiple VLANs, allowing members of multiple VLANs to use the server. Although these VLANs cannot communicate with each other through the server, they can all access the server *over the same connection from the switch*. Where VLANs overlap in this way, VLAN "tags" are used to distinguish between traffic from different VLANs.

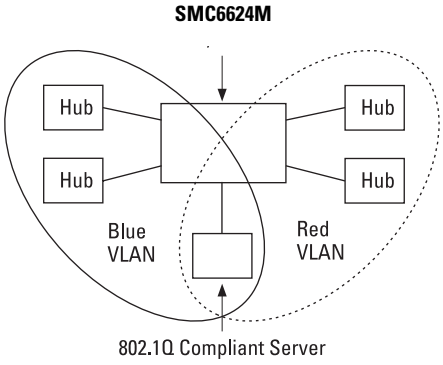



**Figure 9-40. Example of Overlapping VLANs Using the Same Server**

Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through a single switch-to-switch link.

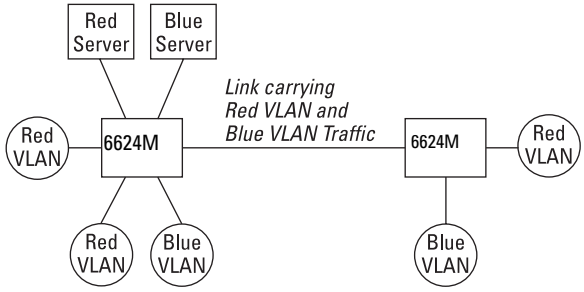



**Figure 9-41. Example of Connecting Multiple VLANs Through the Same Link**

**Introducing Tagged VLAN Technology into Networks Running Legacy (Untagged) VLANs.** You can introduce 802.1Q-compliant devices into networks that have built untagged VLANs based on earlier VLAN technology. The fundamental rule is that legacy/untagged VLANs require a separate link for each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one link. This means that on the 802.1Q-compliant device, separate ports (configured as untagged) must be used to connect separate VLANs to non-802.1Q devices.

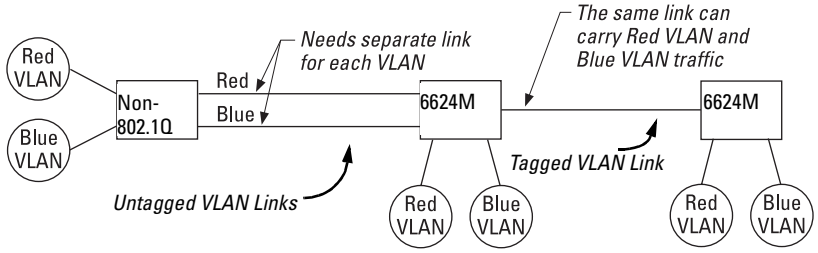



**Figure 9-42. Example of Tagged and Untagged VLAN Technology in the Same Network**

For more information on VLANs, refer to:

- "Overview of Using VLANs" (page 9-51)
- "Menu: Configuring VLAN Parameters (page 9-55)
- "CLI: Configuring VLAN Parameters" ( page 9-55)
- "Web: Viewing and Configuring VLAN Parameters" (page 9-66)
- "VLAN Tagging Information" (page 9-67)
- "Effect of VLANs on Other Switch Features" (page 9-71)
- "VLAN Restrictions" (page 9-73)

# Overview of Using VLANs

## VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the default VLAN (named DEFAULT_VLAN). This places all ports in the switch into one physical broadcast domain. In the factory-default state, the default VLAN is the primary VLAN.

You can partition the switch into multiple virtual broadcast domains by adding one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 30 VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN's VID (which is always "1"). Although you can remove all ports from the default VLAN, this VLAN is always present.

## Which VLAN Is Primary?

Because certain features and management functions, such as single IP-address stacking, run on only one VLAN in the switch, and because DHCP and Bootp can run per-VLAN, there is a need to ensure that multiple instances of

DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch. The *primary* VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch designates the default VLAN (DEFAULT_VLAN) as the primary VLAN. However, to provide more control in your network, you can designate another VLAN as primary. To summarize, *designating a non-default VLAN as primary* means that:

- The stacking feature runs on the switch's designated primary VLAN instead of the default VLAN
- The switch reads DHCP responses on the primary VLAN instead of on the default VLAN.
- The default VLAN continues to operate as a standard VLAN (except, as noted above, you cannot delete it or change its VID).
- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether it is the primary VLAN.

Candidates for primary VLAN include any static VLAN currently configured on the switch. To display the current primary VLAN, use the CLI **show vlan** command.

**Note** If you manually configure a gateway on the switch, it will ignore any gateway address received via DHCP or Bootp.

## Per-Port Static VLAN Configuration Options

The following figure and table show the options you have for assigning individual ports to a static VLAN. Note that GVRP, if configured, affects these options and VLAN behaviour on the switch. The display below shows the per-port VLAN configuration options. Table 9-7 briefly describes these options.

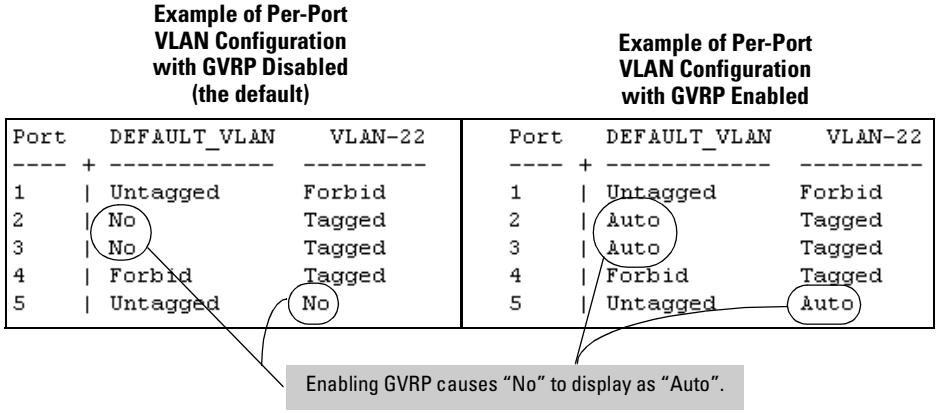



**Figure 9-43. Comparing Per-Port VLAN Options With and Without GVRP**

**Table 9-7. Per-Port VLAN Configuration Options**

| Parameter | Effect on Port Participation in Designated VLAN |
|---|---|
| **Tagged** | Allows the port to join multiple VLANs. |
| **Untagged** | Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN. The switch allows no more than one untagged VLAN assignment per port. |
| **No** *- or -* **Auto** | **No**: Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN.<br>**Auto**: Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID |
| **Forbid** | Prevents the port from joining the VLAN, regardless of whether GVRP is enabled on the switch. |

## General Steps for Using VLANs

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, load balancing, and IGMP. (Refer to "Effect of VLANs on Other Switch Features" on page 9-71.) If you plan on using dynamic VLANs, include the port configuration planning necesary to support this feature. (See "GVRP" on page 9-74.)

   By default, VLAN support is enabled and the switch is configured for eight VLANs.

2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired switch ports to the new VLAN(s).
4. If you are managing VLANs with SNMP in an IP network, each VLAN must have an IP address. Refer to "IP Configuration" on page 5-2.

## Notes on Using VLANs

- If you are using DHCP/Bootp to acquire the switch's configuration, packet time-to-live, and TimeP information, you must designate the VLAN on which DHCP is configured for this purpose as the primary VLAN. (In the factory-default configuration, the DEFAULT_VLAN is the primary VLAN.)
- IGMP, and some other features operate on a "per VLAN" basis. This means you must configure such features separately for each VLAN in which you want them to operate.
- You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.
- Any ports *not* specifically assigned to another VLAN will remain assigned to the DEFAULT_VLAN.
- To delete a VLAN from the switch, you must first remove from that VLAN any ports assigned to it.
- Changing the number of VLANs supported on the switch requires a reboot. Other VLAN configuration changes are dynamic.

# Menu: Configuring VLAN Parameters

In the factory default state, VLAN support is enabled. Also, all ports on the switch belong to the default VLAN (DEFAULT_VLAN) and are in the same broadcast/multicast domain. (The default VLAN is also the default primary VLAN—see "Which VLAN Is Primary?" on page 9-51.) You can configure up to 29 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 30 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP—page 9-74.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See "VLAN Tagging Information" on page 9-67.)

## To Change VLAN Support Settings

This section describes:

- Changing the maximum number of VLANs to support
- Changing the primary VLAN selection (See "Changing the Primary VLAN" on page 9-63.)
- Enabling or disabling dynamic VLANs (See "GVRP" on page 9-74.)

1. From the Main Menu select:

   **2. Switch Configuration**

   **8. VLAN Menu . . .**

   **1. VLAN Support**

   You will then see the following screen:

```
=========================- CONSOLE - MANAGER MODE -============================
                  Switch Configuration - VLAN - VLAN Support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : No

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 9-44. The Default VLAN Support Screen**

2. Press [E] (for **Edit**), then do one or more of the following:

- To change the maximum number of VLANs, type the new number (1 - 30 allowed; default 8).

- To select another primary VLAN, select the **Primary VLAN** field and use the space bar to select from the existing options.
- To enable or disable dynamic VLANs, select the **GVRP Enabled** field and use the Space bar to toggle between options. (For GVRP information, see "GVRP" on page 9-74.)

**Note**

For optimal switch memory utilization, set the number of VLANs at the number you will likely be using or a few more. If you need more VLANs later, you can increase this number, but a switch reboot will be required at that time.

3. Press [Enter] and then [S] to save the VLAN support configuration and return to the VLAN Menu screen.

   If you changed the value for **Maximum VLANs to support**, you will see an asterisk next to the **VLAN Support** option (see below).

An asterisk indicates you must reboot the switch to implement the new Maximum VLANs setting.

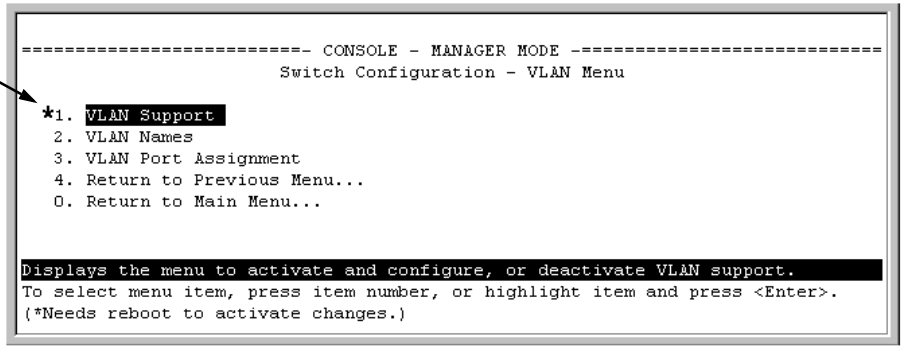



**Figure 9-45. VLAN Menu Screen Indicating the Need To Reboot the Switch**

   – If you changed the VLAN Support option, you must reboot the switch before the Maximum VLANs change can take effect. You can go on to configure other VLAN parameters first, but remember to reboot the switch when you are finished.
   – If you did not change the VLAN Support option, a reboot is not necessary.

4. Press [0] to return to the Main Menu.

## Adding or Editing VLAN Names

Use this procedure to add a new VLAN or to edit the name of an existing VLAN.

1. From the Main Menu select:

   **2. Switch Configuration**
   **8. VLAN Menu . . .**
   **2. VLAN Names**

   If multiple VLANs are not yet configured you will see a screen similar to figure 9-46:

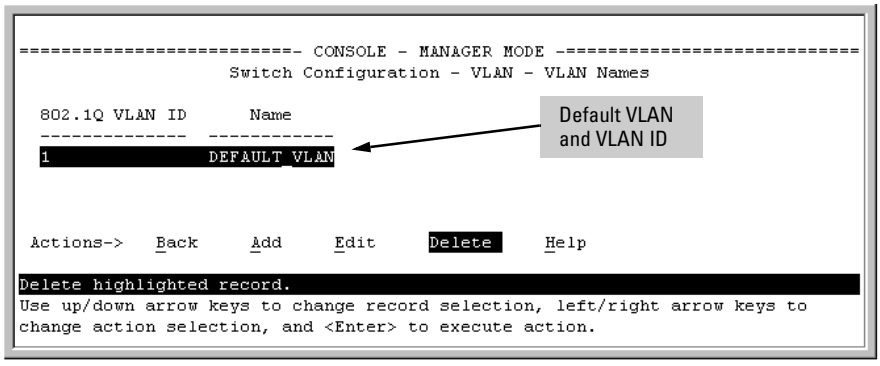



**Figure 9-46. The Default VLAN Names Screen**

2. Press [A] (for **Add**). You will then be prompted for a new VLAN name and VLAN ID:

   **802.1Q VLAN ID : 1**
   **Name : _**

3. Type in a VID (VLAN ID number). This can be any number from 2 to 4095 that is not already being used by another VLAN.

   Remember that a VLAN *must* have the same VID in every switch in which you configure that same VLAN. (You can use GVRP to dynamically extend VLANs with correct VID numbering to other switches. See "GVRP" on page 9-74.)

4. Press [↓] to move the cursor to the **Name** line and type the VLAN name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press [Enter].

5. Press [S] (for **Save**). You will then see the VLAN Names screen with the new VLAN listed.

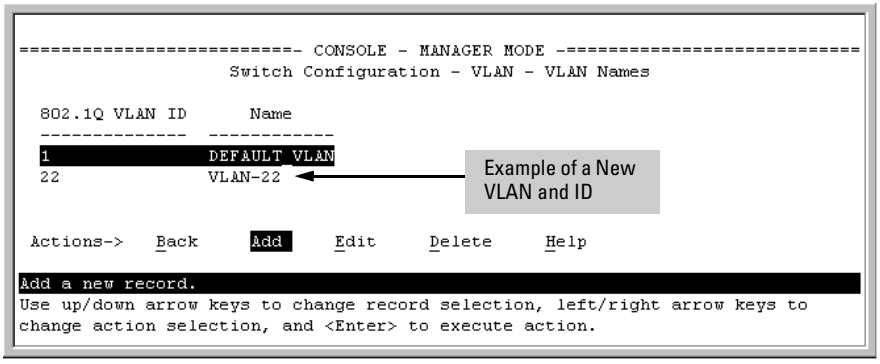



**Figure 9-47. Example of VLAN Names Screen with a New VLAN Added**

6. Repeat steps 2 through 5 to add more VLANs.

   Remember that you can add VLANs until you reach the number specified in the **Maximum VLANs to support** field on the VLAN Support screen (see figure 9-44on page 9-55). This includes any VLANs added dynamically due to GVRP operation.

7. Return to the VLAN Menu to assign ports to the new VLAN(s) as described in the next section, “Adding or Changing a VLAN Port Assignment”.

## Adding or Changing a VLAN Port Assignment

Use this procedure to add ports to a VLAN or to change the VLAN assignment(s) for any port. (Ports not specifically assigned to a VLAN are automatically in the default VLAN.)

1. From the Main Menu select:

   **2. Switch Configuration**

   **8. VLAN Menu . . .**

   **3. VLAN Port Assignment**

   You will then see a VLAN Port Assignment screen similar to the following:

**Default:** In this example, the "VLAN-22" has been defined, but no ports have yet been assigned to it. ("No" means the port is not assigned to that VLAN.)
**Using GVRP?** If you plan on using GVRP, any ports you don't want to join should be changed to "Forbid".

A port can be assigned to several VLANs, but only one of those assignments can be "Untagged".

```
=========================- CONSOLE - MANAGER MODE -==============================
                Switch Configuration - VLAN - VLAN Port Assignment

  Port   DEFAULT_VLAN    VLAN-22      |  Port   DEFAULT_VLAN    VLAN-22
  ---- + ------------  ------------   |  ---- + ------------  ------------
  1    | Untagged      No             |  8    | Untagged      No
  2    | Tagged        No             |  9    | Untagged      No
  3    | Untagged      No             |  10   | Untagged      No
  4    | Untagged      No             |  11   | Untagged      No
  5    | Untagged      No             |  12   | Untagged      No
  6    | Untagged      No             |  13   | Untagged      No
  7    | Untagged      No             |  14   | Untagged      No

 Actions->   Cancel    Edit    Save    Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 9-48. Example of VLAN Port Assignment Screen**

2. To change a port's VLAN assignment(s):
   a. Press [E] (for **Edit**).
   b. Use the arrow keys to select a VLAN assignment you want to change.
   c. Press the Space bar to make your assignment selection (**No**, **Tagged**, **Untagged**, or **Forbid**).

**Note**

**For GVRP Operation:** If you enable GVRP on the switch, "**No**" converts to "**Auto**", which allows the VLAN to dynamically join an advertised VLAN that has the same VID. See "Per-Port Options for Dynamic VLAN Advertising and Joining" on page 9-79.

**Untagged VLANs**: Only one untagged VLAN is allowed per port. Also, there must be at least one VLAN assigned to each port. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN).

For example, if you want ports 4 and 5 to belong to both DEFAULT_VLAN and VLAN-22, and ports 6 and 7 to belong only to VLAN-22, you would use the settings in figure 9-49. (This example assumes the default GVRP setting—disabled—and that you do not plan to enable GVRP later.)

Ports 4 and 5 are assigned to both VLANs.

Ports 6 and 7 are assigned only to VLAN-22.

All other ports are assigned only to the Default VLAN.

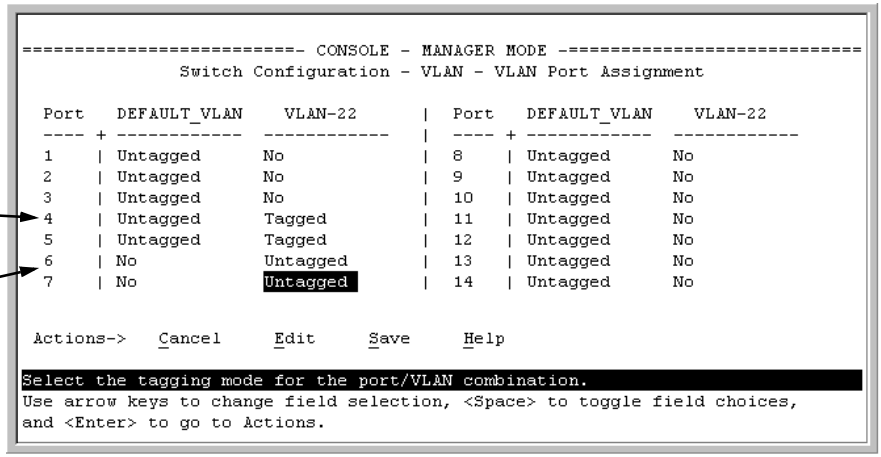



**Figure 9-49. Example of VLAN Assignments for Specific Ports**

For information on VLAN tags ("Untagged" and "Tagged"), refer to "VLAN Tagging Information" on page 9-67.

d. If you are finished assigning ports to VLANs, press [Enter] and then [S] (for **Save**) to activate the changes you've made and to return to the Configuration menu. (The console then returns to the VLAN menu.)

3. Return to the Main menu.

## CLI: Configuring VLAN Parameters

In the factory default state, all ports on the switch belong to the default VLAN (DEFAULT_VLAN) and are in the same broadcast/multicast domain. (The default VLAN is also the default primary VLAN—see "Which VLAN Is Primary?" on page 9-51.) You can configure up to 29 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 30 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP—page 9-74.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See "VLAN Tagging Information" on page 9-67.)

**VLAN Commands Used in this Section**

| | |
|---|---|
| show vlans | below |
| show vlan <*vlan-id*> | page 9-62 |
| max-vlans <1..30> | page 9-63 |
| primary-vlan <*vlan-id*> | page 9-63 |
| [no] vlan <*vlan-id*> | page 9-64 |
| name <*vlan-name*> | page 9-65 |
| [no] tagged <*port-list*> | page 9-65 |
| [no] untagged <*port-list*> | page 9-65 |
| [no] forbid | page 9-65 |
| auto <*port-list*> | page 9-65 (Available if GVRP enabled.) |
| static-vlan <*vlan-id*> | page 9-65 (Available if GVRP enabled.) |



**Displaying the Switch's VLAN Configuration.** The next command lists the VLANs currently running in the switch, with VID, VLAN name, and VLAN status. Dynamic VLANs appear only if the switch is running with GVRP enabled and one or more ports has dynamically joined an advertised VLAN. (In the default configuration, GVRP is disabled. (See "GVRP" on page 9-74.)

***Syntax:*** show vlan

```
Status and Counters - VLAN Information
 VLAN support : Yes
 Maximum VLANs to support : 8
 Primary VLAN : DEFAULT_VLAN

 802.1Q VLAN ID Name           Status
 -------------- -------------- --------------
 1              DEFAULT_VLAN   Static
 22             VLAN-22        Static
 33             GVRP_33        Dynamic
```

When GVRP is disabled (the default), Dynamic VLANs do not exist on the switch and do not appear in this listing. (See "GVRP" on page 9-74.)

**Figure 9-50. Example of "Show VLAN" Listing (GVRP Enabled)**

**Displaying the Configuration for a Particular VLAN .** This command uses the VID to identify and display the data for a specific static or dynamic VLAN.

***Syntax:*** show vlan <*vlan-id*>

```
SMC TigerSwitch 10/100# show vlan 22
 Status and Counters - VLAN Information - Ports - VLAN 22

  802.1Q VLAN ID : 22
  Name           : VLAN-22
  Status         : Static

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                Tagged   Learn        Up
  2                Tagged   Learn        Up
  5                Untagged Learn        Up
  6                Untagged Learn        Up
  7                Untagged Learn        Up
```

**Figure 9-51. Example of "Show VLAN" for a Specific Static VLAN**

**Show VLAN** lists this data when GVRP is enabled and at least one port on the switch has dynamically joined the designated VLAN.

```
SMC TigerSwitch 10/100# show vlan 44
 Status and Counters - VLAN Information - Ports - VLAN 44
  802.1Q VLAN ID : 44
  Name           : GVRP_44
  Status         : Dynamic

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  6                Auto     Learn        Up
```

**Figure 9-52. Example of "Show VLAN" for a Specific Dynamic VLAN**

**Changing the Number of VLANs Allowed on the Switch.** By default, the switch allows a maximum of 8 VLANs. You can specify any value from 1 to 30. (If GVRP is enabled, this setting includes any dynamic VLANs on the switch.) As part of implementing a new value, you must execute a write memory command (to save the new value to the startup-config file) and then reboot the switch.

***Syntax:*** max-vlans <1 .. 30>

For example, to reconfigure the switch to allow 10 VLANs:

```
SMC TigerSwitch 10/100# config
SMC TigerSwitch 10/100(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
SMC TigerSwitch 10/100(config)# write memory
SMC TigerSwitch 10/100(config)# boot
Device will be rebooted, do you want to continue [y/n]?
```

Note that you can execute these three steps at another time.

**Figure 9-53. Example of Command Sequence for Changing the Number of VLANs**

**Changing the Primary VLAN.** In the factory-default configuration, the default VLAN (DEFAULT_VLAN) is the primary VLAN. However, you can designate any static VLAN on the switch as the primary VLAN. (For more on the primary VLAN, see "Which VLAN Is Primary?" on page 9-51.) To view the available VLANs and their respective VIDs, use **show vlan**.

***Syntax:*** primary-vlan <*vlan-id*>

For example, to make VLAN 22 the primary VLAN:

```
SMC TigerSwitch 10/100(config)# primary-vlan 22
```

### Creating a New Static VLAN
### Changing the VLAN Context Level.

With this command, entering a new VID creates a new static VLAN. Entering the VID or name of an existing static VLAN places you in the context level for that VLAN.

***Syntax:*** vlan <*vlan-id*> [name <*name-str*>] Creates a new static VLAN if a VLAN with that VID does not already exist, and places you in that VLAN's context level. If you do not use the name option, the switch uses "VLAN" and the new VID to automatically name the VLAN.
If the VLAN already exists, the switch places you in the context level for that VLAN.

vlan <*vlan-name*> Places you in the context level for that static VLAN.

For example, to create a new static VLAN with a VID of 100:

```
SMC TigerSwitch 10/100(config)# vlan 100
100: VLAN added.
SMC TigerSwitch 10/100(vlan-100)# show vlan

 Status and Counters - VLAN Information

  VLAN support : Yes
  Maximum VLANs to support : 10
  Primary VLAN : DEFAULT_VLAN

  802.1Q VLAN ID Name          Status
  -------------- ------------- -------------
  1              DEFAULT_VLAN  Static
  100            VLAN100       Static
```

Creating the new VLAN.
Showing the result.

To go to a different VLAN context level, such as to the default VLAN:

```
SMC TigerSwitch 10/100(vlan-100)# vlan default_vlan
SMC TigerSwitch 10/100(vlan-1) _
```

**Converting a Dynamic VLAN to a Static VLAN.** If GVRP is running on the switch and a port dynamically joins a VLAN, you can use the next command to convert the dynamic VLAN to a static VLAN. (For GVRP and dynamic VLAN operation, see "GVRP" on page 9-74.) This is necessary if you want to make the VLAN permanent. Note that after you convert a dynamic VLAN to static, you must configure the switch's per-port participation in the VLAN in the same way that you would for any static VLAN.

***Syntax:*** static-vlan <*vlan-id*>

If you need a VID reference, use **show vlan** to list the switch's currently existing VLANs.

For example, suppose a dynamic VLAN with a VID of 125 exists on the switch. The following command converts the VLAN to a static VLAN.

```
SMC TigerSwitch 10/100(config)# static-vlan 125
```

**Configuring Static VLAN Name and Per-Port Settings.** The **vlan <*vlan-id*>** command, used in conjunction with the options listed below, enables you to change the name of an existing static VLAN and change the per-port VLAN membership settings as show below.

**Note**

You can use these options from the configuration level by beginning the command with **vlan <*vlan-id*>**, or from the context level of the specific VLAN.

| | | |
|---|---|---|
| ***Syntax:*** | name <*vlan-name*> | Changes the name of the existing static VLAN. (No spaces allowed in the <*vlan-name*> entry. |
| | [no] tagged <*port-list*> | Configures the indicated port(s) as **Tagged** for the specified VLAN. The "**no**" version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**. |
| | [no] untagged <*port-list*> | Configures the indicated port(s) as **Untagged** for the specified VLAN. The "**no**" version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**. |
| | [no] forbid <*port-list*> | Configures the indicated port(s) as "forbidden" to participate in the designated VLAN. The "**no**" version sets the port(s) to either **No** or (if GVRP is enabled) to **Auto**. |
| | auto <*port-list*> | Available if GVRP is enabled on the switch. Returns the per-port settings for the specified VLAN to **Auto** |

operation. Note that **Auto** is the default per-port setting for a static VLAN if GVRP is runing on the switch.

(For information on dynamic VLAN and GVRP operation, see "GVRP" on page 9-74.)

For example, suppose you have a VLAN named VLAN100 with a VID of 100, and all ports are set to No for this VLAN. To change the VLAN name to "Blue_Team" and set ports 1-5 to Tagged, you could do so with these commands:

```
SMC TigerSwitch 10/100(config)# vlan 100 name Blue_Team
SMC TigerSwitch 10/100(config)# vlan 100 tagged 1-5
```

To move to the vlan 100 context level and execute the same commands:

```
SMC TigerSwitch 10/100(config)# vlan 100
SMC TigerSwitch 10/100(vlan-100)# name Blue_Team
SMC TigerSwitch 10/100(vlan-100)# tagged 1-5
```

Similarly, to change the tagged ports in the above examples to **No** (or **Auto**, if GVRP is enabled), you could use either of the following commands.

At the config level, use:

```
SMC TigerSwitch 10/100(config)# no vlan 100 tagged 1-5
```

*- or -*

At the VLAN 100 context level, use:

```
SMC TigerSwitch 10/100(vlan-100)# no tagged 1-5
```

**Note** You cannot use these commands with dynamic VLANs. Attempting to do so results in the message "**VLAN already exists.**" and no change occurs.

## Web: Viewing and Configuring VLAN Parameters

In the web browser interface you can do the following:

- Add VLANs
- Rename VLANs
- Remove VLANs
- Configure GVRP security
- Select a new Primary VLAN

To configure static VLAN port parameters, you will need to use the menu interface (available by Telnet from the web browser interface) or the CLI.

1. Click on the Configuration tab.
2. Click on [VLAN Configuration].
3. Click on [Add/Remove VLANs].

## VLAN Tagging Information

VLAN tagging enables traffic from more than one VLAN to use the same port. (Even when two or more VLANs use the same port they remain as separate domains and cannot receive traffic from each other without going through an external router.) As mentioned earlier, a "tag" is simply a unique VLAN identification number (VLAN ID, or VID) assigned to a VLAN at the time that you configure the VLAN name in the switch. In the SMC6624M switch the tag can be any number from 1 to 4095 that is not already assigned to a VLAN. When you subsequently assign a port to a given VLAN, you must implement the VLAN tag (VID) if the port will carry traffic for more than one VLAN. Otherwise, the port VLAN assignment can remain "untagged" because the tag is not needed. On a given switch, this means you should use the "Untagged" designation for a port VLAN assignment where the port is connected to non 802.1Q-compliant device or is assigned to only one VLAN. Use the "Tagged" designation when the port is assigned to more than one VLAN or the port is connected to a device that *does* comply with the 802.1Q standard.

For example, if port 7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain "untagged" because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port 7, then at least one of those VLAN assignments must be "tagged" so that Red VLAN traffic can be distinguished from Green VLAN traffic. The following illustration shows this concept:

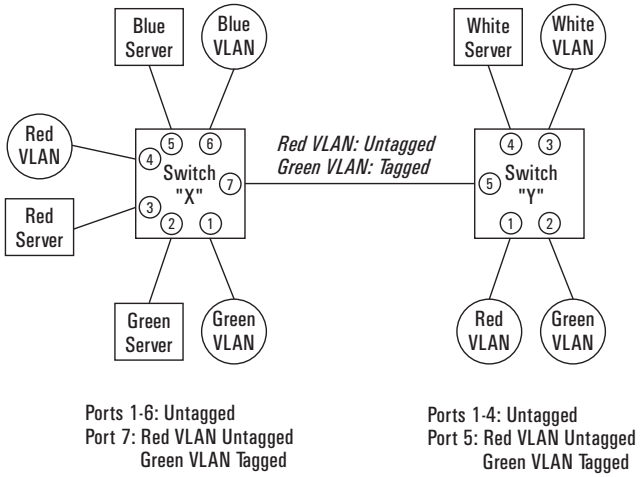



**Figure 9-54. Example of Tagged and Untagged VLAN Port Assignments**

- In switch X:
  - VLANs assigned to ports X1 - X6 can all be untagged because there is only one VLAN assignment per port. Red VLAN traffic will go out only the Red ports; Green VLAN traffic will go out only the Green ports, and so on. Devices connected to these ports do not have to be 802.1Q-compliant.
  - However, because both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.
- In switch Y:
  - VLANs assigned to ports Y1 - Y4 can all be untagged because there is only one VLAN assignment per port. Devices connected to these ports do not have to be 802.1Q-compliant.
  - Because both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port.
- In both switches: The ports on the link between the two switches must be configured the same. As shown in figure 9-54 (above), the Red VLAN must be untagged on port X7 and Y5 and the Green VLAN must be tagged on port X7 and Y5, or vice-versa.

**Note**

Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN *must* be given the same VID in every device in which it is configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be used for the Red VID in switch Y.



VID Numbers

```
==========================- CONSOLE - MANAGER MODE -=============================
                    Switch Configuration - VLAN - VLAN Names

  802.1Q VLAN ID      Name
  --------------  ------------
  1               DEFAULT_VLAN
  10              Red_VLAN
  20              Blue_VLAN


 Actions->   Back     Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 9-55. Example of VLAN ID Numbers Assigned in the VLAN Names Screen**

VLAN tagging gives you several options:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as "Untagged" (the default).
- Any port that has two or more VLANs assigned to it can have one VLAN assignment for that port as "Untagged". All other VLANs assigned to the same port must be configured as "Tagged". (There can be no more than one Untagged VLAN on a port.)
- If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, then, you can configure all VLAN assignments on a port as "Tagged" if doing so makes it easier to manage your VLAN assignments, or for security reasons.

For example, in the following network, switches X and Y and servers S1 and S2 are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.)

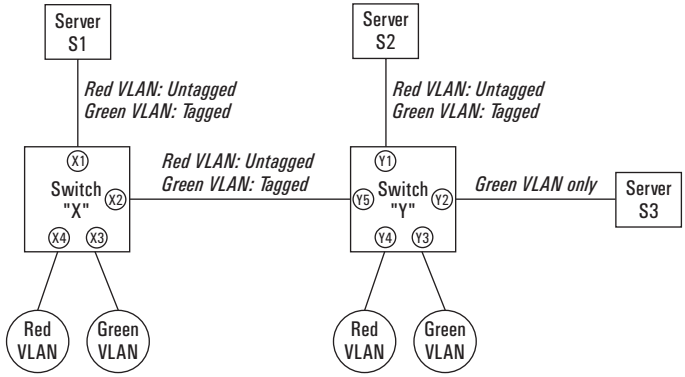



**Figure 9-56. Example of Networked 802.1Q-Compliant Devices with Multiple VLANs on Some Ports**

The VLANs assigned to ports X3, X4, Y2, Y3, and Y4 can all be untagged because there is only one VLAN assigned per port. Port X1 has multiple VLANs assigned, which means that one VLAN assigned to this port can be untagged and any others must be tagged. The same applies to ports X2, Y1, and Y5.

| Switch X | | | Switch Y | | |
|---|---|---|---|---|---|
| **Port** | **Red VLAN** | **Green VLAN** | **Port** | **Red VLAN** | **Green VLAN** |
| X1 | Untagged | Tagged | Y1 | Untagged | Tagged |
| X2 | Untagged | Tagged | Y2 | No* | Untagged |
| X3 | No* | Untagged | Y3 | No* | Untagged |
| X4 | Untagged | No* | Y4 | Untagged | No* |
| | | | Y5 | Untagged | Tagged |

*"No" means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic. Also, if GVRP were enabled, "Auto" would appear instead of "No".

**Note**

VLAN configurations on ports connected by the same link must match. Because ports X2 and Y5 are opposite ends of the same point-to-point connection, both ports must have the same VLAN configuration; that is, both ports configure the Red VLAN as "Untagged" and the Green VLAN as "Tagged".

To summarize:

| VLANs Per Port | Tagging Scheme |
|---|---|
| 1 | Untagged or Tagged. If the device connected to the port is 802.1Q-compliant, then the recommended choice is "Tagged". |
| 2 or More | 1 VLAN Untagged; all others Tagged<br>or<br>All VLANs Tagged |
| A given VLAN *must* have the same VID on any 802.1Q-compliant device in which the VLAN is configured.<br>The ports connecting two 802.1Q devices should have identical VLAN configurations, as shown for ports X2 and Y5, above. | |



# Effect of VLANs on Other Switch Features

## Spanning Tree Protocol Operation with VLANs

Because the SMC6624M switch follows the 802.1Q VLAN recommendation to use single-instance spanning tree, STP operates across all ports on the switch (regardless of VLAN assignments) instead of on a per-VLAN basis. This means that if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, regardless of whether the redundant links are in separate VLANs. However, you can use port trunking to prevent STP from unnecessarily blocking ports (and to improve overall network performance). Refer to "STP Operation with 802.1Q VLANs" on page 9-107.

Note that STP operates differently in different devices. For example, in some switches, STP operates on a per-VLAN basis, allowing redundant physical links as long as they are in separate VLANs.

## IP Interfaces

There is a one-to-one relationship between a VLAN and an IP network interface. Since the VLAN is defined by a group of ports, the state (up/down) of those ports determines the state of the IP network interface associated with that VLAN. When a VLAN comes up because one or more of its ports is up, the IP interface for that VLAN is also activated. Likewise, when a VLAN is deactivated because all of its ports are down, the corresponding IP interface is also deactivated.

## VLAN MAC Addresses

The switch has one unique MAC address for each of its VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch. Likewise, you can assign an IP address to the VLAN interface, and when you Ping that address, ARP will resolve the IP address to this MAC address. The switch allows up to 30 VLAN MAC addresses (one per possible VLAN).

## Port Trunks

When assigning a port trunk to a VLAN, all ports in the trunk are automatically assigned to the same VLAN. You cannot split trunk members across multiple VLANs. Also, a port trunk is tagged, untagged, or excluded from a VLAN in the same way as for individual, untrunked ports.

## Port Monitoring

If you designate a port on the switch for network monitoring, this port will appear in the Port VLAN Assignment screen and can be configured as a member of any VLAN. For information on how broadcast, multicast, and unicast packets are tagged inside and outside of the VLAN to which the monitor port is assigned, see “VLAN-Related Problems” on page 11-8.

## VLAN Restrictions

- A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN; VID = 1).
- A port can be assigned to several VLANs, but only one of those assignments can be untagged. (The "Untagged" designation enables VLAN operation with non 802.1Q-compliant devices.)
- An external router must be used to communicate between tagged VLANs.
- Duplicate MAC addresses on different VLANs are not supported and can cause VLAN operating problems. These duplicates are possible and common in situations involving Sun workstations with multiple network interface cards, with DECnet routers, and with certain routers where any of the following are enabled:
  - IPX
  - IP Host-Only
  - STP
  - XNS
  - DECnet

  Currently, for the problem of duplicate MAC addresses in XNS and DECnet environments, a satisfactory solution is not available from any vendor at this time.

**Note**

Operating problems associated with duplicate MAC addresses are likely to occur in VLAN environments where XNS and DECnet are used. For this reason, using VLANs in XNS and DECnet environments is not currently supported.

- Before you can delete a VLAN, you must first re-assign all ports in the VLAN to another VLAN.

### Symptoms of Duplicate MAC Addresses in VLAN Environments

There are no definitive events or statistics to indicate the presence of duplicate MAC addresses in a VLAN environment. However, one symptom that may occur is that the duplicate MAC address can be seen in the Port Address Table for more than one port. You can do a search for the suspected MAC address in the switch's address table and if there is a duplicate MAC address problem, the address will be found in the table associated with one port at one moment, and then later associated with a different port.

# GVRP

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view GVRP configuration | n/a | page 9-81 | page 9-83 | page 9-86 |
| list static and dynamic VLANs on a GVRP-enabled switch | n/a | — | page 9-85 | page 9-86 |
| enable or disable GVRP on the switch | disabled | page 9-81 | page 9-84 | page 9-86 |
| enable or disable GVRP on individual ports | enabled | page 9-81 | page 9-84 | — |
| control how individual ports will handle advertisements for new VLANs | Learn | page 9-81 | page 9-84 | page 9-86 |
| convert a dynamic VLAN to a static VLAN | n/a | — | page 9-86 | — |
| configure static VLANs | DEFAULT_VLAN (VID = 1) | page 9-55 | page 9-60 | page 9-86 |

GVRP—GARP VLAN Registration Protocol—is an application of the Generic Attribute Registration Protocol—GARP. GVRP is defined in the IEEE 802.1Q standard, and GARP is defined in the IEEE 802.1P standard.

**Note**

To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (See "Port-Based Virtual LANs (Static VLANs)" on page 9-48.)

GVRP uses "GVRP Bridge Protocol Data Units" ("GVRP BPDUs") to "advertise" static VLANs. In this manual, a GVRP BPDU is termed an *advertisement*.

GVRP enables the SMC6624M to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across your network. After the switch creates a dynamic VLAN, you can optionally use the CLI **static <*vlan-id*>** command convert it to a static VLAN or allow it to continue as a dynamic VLAN for as long as needed. You can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.

**Note**

There must be one common VLAN (that is, one common VID) connecting all of the GVRP-aware devices in the network to carry GVRP packets. SMC recommends the default VLAN (DEFAULT_VLAN; VID = 1), which is automatically enabled and configured as untagged on every port of the SMC6624M switch). That is, on ports used for GVRP links, leave the default VLAN set to **Untagged** and configure other static VLANs on the same ports as either **Tagged**, **Auto**, or **Forbid**. (**Auto** and **Forbid** are described under "Per-Port Options for Dynamic VLAN Advertising and Joining" on page 9-79.

## General Operation

A GVRP-enabled port with a Tagged or Untagged static VLAN sends advertisements (BPDUs, or Bridge Protocol Data Units) advertising the VLAN (actually, its VID). Another GVRP-aware port receiving the advertisements over a link can dynamically join the advertised VLAN. *All dynamic VLANs operate as Tagged VLANs*. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch. However, the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received on that specific port.

Core switch with static VLANs (VID= 1, 2, & 3). Port 2 is a member of VIDs 1, 2, & 3.

**1.** Port 2 advertises VIDs 1, 2, & 3.

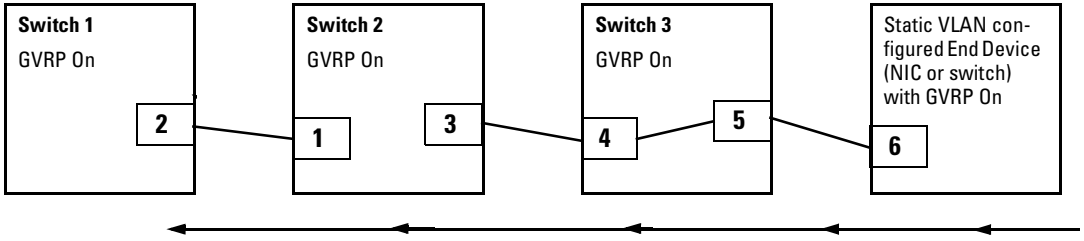
**2.** Port 1 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

**3.** Port 3 advertises VIDs 1, 2, & 3, but port 3 is NOT a member of VIDs 1, 2, & 3 at this point.

**4.** Port 4 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

**5.** Port 5 advertises VIDs 1, 2, & 3, but port 5 is NOT a member of VIDs 1, 2, & 3 at this point.

Port 6 is statically configured to be a member of VID 3.




**11.** Port 2 receives advertisement of VID 3. (Port 2 is already statically configured for VID 3.

**9.** Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)

**10.** Port 1 advertises VID 3.

**7.** Port 5 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 & 2.)

**8.** Port 4 advertises VID 3.

**6.** Port 6 advertises VID 3.

**Figure 9-57. Example of Forwarding Advertisements and Dynamic Joining**

Note that if a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

For example, in the following figure, Tagged VLAN ports on switch "A" and switch "C", below advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.

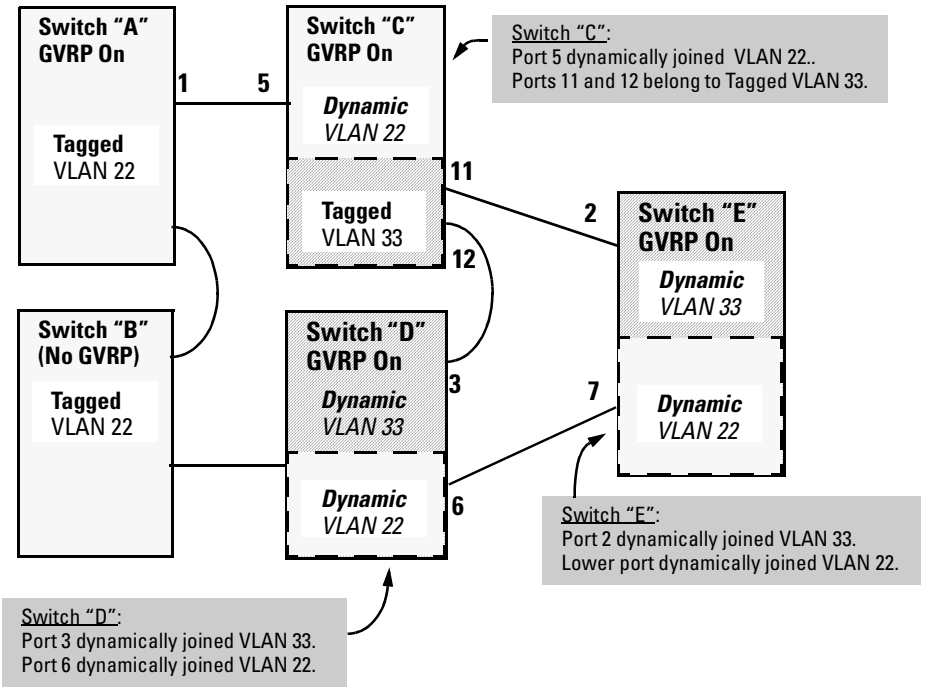



**Figure 9-58. Example of GVRP Operation**

**Note**

A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch "B", above). VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through.

A GVRP-aware port receiving advertisements has these options:

- If there is not already a static VLAN with the advertised VID on the receiving port, then dynamically create a VLAN with the same VID as in the advertisement, and begin moving that VLAN's traffic.

- If the switch already has a static VLAN assignment with the same VID as in the advertisement, and the port is configured to **Auto** for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN's traffic. (For more detail on **Auto**, see "Per-Port Options for Dynamic VLAN Advertising and Joining" on page 9-79.)
- Ignore the advertisement for that VID and drop all GVRP traffic with that VID.
- Don't participate in that VLAN.

Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:

- Send VLAN advertisements, and also receive advertisements for VLANs on other ports and dynamically join those VLANs.
- Send VLAN advertisements, but ignore advertisements received from other ports.
- Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices.

**IP Addressing.** A dynamic VLAN does not have an IP address, and moves traffic on the basis of port membership in VLANs. However, after GVRP creates a dynamic VLAN, you can convert it to a static VLAN. Note that it is then necessary to assign ports to the VLAN in the same way that you would for a static VLAN that you created manually. In the static state you can configure IP addressing on the VLAN and access it in the same way that you would any other static (manually created) VLAN.

## Per-Port Options for Handling GVRP "Unknown VLANs"

An "unknown VLAN" is a VLAN that the switch learns of by GVRP. For example, suppose that in figure 9-58 (page 9-76), port 1 on switch "A" is connected to port 5 on switch "C". Because switch "A" has VLAN 22 statically configured, while switch "C" does not have this VLAN statically configured, VLAN 22 is handled as an "Unknown VLAN" on port 5 in switch "C". Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch "A".

When you enable GVRP on a switch, you have the per-port join-request options listed in table 9-8:

**Table 9-8. Options for Handling "Unknown VLAN" Advertisements:**

| Unknown VLAN Mode | Operation |
|---|---|
| Learn (the Default) | Enables the port to dynamically join any VLAN for which it receives an advertisement, and allows the port to forward advertisements it receives. |
| Block | Prevents the port from dynamically joining a VLAN that is not statically configured on the switch. The port will still forward advertisements that were received by the switch on other ports. Block should typically be used on ports in unsecure networks, where there is exposure to "attacks", such as ports where intruders can connect. |
| Disable | Causes the port to ignore and drop all advertisements it receives from any source. |

The CLI **show gvrp** command and the menu interface VLAN Support screen show a switch's current GVRP configuration, including the Unknown VLAN settings.

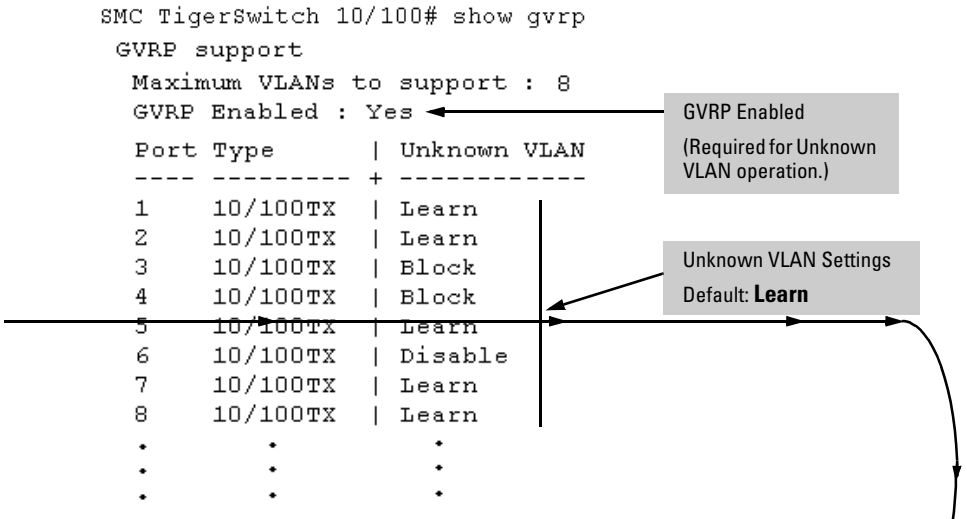



**Figure 9-59. Example of GVRP Unknown VLAN Settings**

The above options also influence GVRP operation on ports where static VLANs are configured. (See the next section.)

## Per-Port Options for Dynamic VLAN Advertising and Joining

**Initiating Advertisements.** As described in the preceding section, to enable dynamic joins, GVRP must be enabled and a port must be configured to Learn (the default). However, to send advertisements in your network, one or more Tagged or Untagged static VLANs must be configured on one or more switches (with GVRP enabled), depending on your topology.

**Enabling a Static VLAN for Dynamic Joins.** You can configure a port to dynamically join a static VLAN (that shares the same VID) if that port subsequently receives an advertisement for the static VLAN. (This is done by using the **Auto** and **Learn** options described in table 9-9, below.

**Parameters for Controlling VLAN Propagation Behavior.** On an individual port, you can configure an existing static VLAN to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP "Unknown VLAN" and the static VLAN configuration parameters, as described in the following table:

**Table 9-9. Controlling VLAN Behavior on Ports with Static VLANs**

| Per-Port "Unknown VLAN" (GVRP) Configuration | Per-Port Static VLAN Options [1] | | |
|---|---|---|---|
| | **Tagged or Untagged[2]** | **Auto[2]** | **Forbid[2]** |
| Learn<br>(the Default) | Generate advertisements.<br>Forward advertisements for other VLANs.<br>Receive advertisements and dynamically join any advertised VLAN. | Receive advertisements and dynamically join any advertised VLAN that has the same VID as the static VLAN. | Do not allow the port to become a member of this VLAN. |
| Block | Generate advertisements.<br>Forward advertisements received from other ports for other VLANs.<br>Do not dynamically join any advertised VLAN. | Receive advertisements and dynamically join any advertised VLAN that has the same VID. | Do not allow the VLAN on this port. |
| Disable | Ignore GVRP and drop all GVRP advertisements. | Ignore GVRP and drop all GVRP advertisements. | Do not allow the VLAN on this port. |

[1] Each port of an SMC6624M switch must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for the static VLAN(s) for which it has been configured as Tagged or Untagged . By default, all ports are Untagged members of the default VLAN (VID = 1). See the "Note" on page page 9-75.

[2] To configure tagging, **Auto**, or **Forbid**, see "Configuring Static VLAN Name and Per-Port Settings" on page 9-65 (for the CLI) or "Adding or Changing a VLAN Port Assignment" on page 9-58 (for the menu).

As the above table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

**Note**

In table 9-9, above, the Unknown VLAN parameters are configured on a per-interface basis using the CLI. The Tagged, Untagged, Auto, and Forbid options are configured in the VLAN context using either the menu interface or the CLI.

Because dynamic VLANs operate as Tagged VLANs, and because a tagged port on one device cannot communicate with an untagged port on another device, SMC recommends that you use Tagged VLANs for the static VLANs you will use to generate advertisements.

## GVRP and VLAN Access Control

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch's ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:

- Allow a port to advertise and/or join dynamic VLANs (the default).
- Allow a port to send VLAN advertisements, but not receive them from other devices; that is, the port cannot dynamically join a VLAN but other devices can dynamically join the VLANs it advertises.
- Prevent a port from sending dynamic VLAN advertisements for specific VLANs
- Prevent a port from participating in GVRP operation.

### Port-Leave From a Dynamic VLAN

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN (See "Converting a Dynamic VLAN to a Static VLAN" on page 9-65.)
- Reconfigure the port to **Block** or **Disable**
- Disable GVRP
- Reboot the switch
- The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

## Planning for GVRP Operation

These steps outline the procedure for setting up dynamic VLANs for a segment.

1. Determine the VLAN topology you want for each segment (broadcast domain) on your network.
2. Determine the VLANs that must be static and the VLANs that can be dynamically propagated.
3. Determine the device or devices on which you must manually create static VLANs in order to propagate VLANs throughout the segment.
4. Determine security boundaries and how the individual ports in the segment will handle dynamic VLAN advertisements. (See table 9-8 on page 9-78 and table 9-9 on page 9-79.)
5. Enable GVRP on all devices you want to use with dynamic VLANs and configure the appropriate "Unknown VLAN" parameter (**Learn**, **Block**, or **Disable**) for each port.
6. Configure the static VLANs on the switch(es) where they are needed, along with the per-VLAN parameters (**Tagged**, **Untagged**, **Auto**, and **Forbid**—see table 9-9 on page 9-79) on the appropriate ports.
7. Dynamic VLANs will then appear automatically, according to the configuration options you have chosen.
8. Convert dynamic VLANs to static VLANs where you want dynamic VLANs to become permanent.

## Configuring GVRP On a Switch

The procedures in this section describe how to:

- View the GVRP configuration on a switch
- Enable and disable GVRP on a switch
- Specify how individual ports will handle advertisements

To view or configure static VLANs for GVRP operation, refer to "Port-Based Virtual LANs (Static VLANs)" on page 9-48.

### Menu: Viewing and Configuring GVRP

1. From the Main Menu, select:

**2. Switch Configuration . . .**
**8. VLAN Menu . . .**
**1. VLAN Support**

```
==========================- CONSOLE - MANAGER MODE -============================
                    Switch Configuration - VLAN - VLAN Support

  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : No


 Actions->   Cancel     Edit      Save      Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 9-60. The VLAN Support Screen (Default Configuration)**

2. Do the following to enable GVRP and display the Unknown VLAN fields:
   a. Press [E] (for **Edit**).
   b. Use [↓] to move the cursor to the **GVRP Enabled** field.
   c. Press the Space bar to select **Yes**.
   d. Press [↓] again to display the **Unknown VLAN** fields.

The Unknown VLAN fields enable you to configure each port to:
- Learn - Dynamically join any advertised VLAN and forward all advertisements the port receives.
- Block - Do not dynamically join any VLAN, but still forward advertisements.
- Disable - Ignore and drop all advertisements.

```
==========================- CONSOLE - MANAGER MODE -============================
                    Switch Configuration - VLAN - VLAN Support
  Maximum VLANs to support [8] : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled [No] : Yes

  Port    Type       Unknown VLAN   |  Port    Type       Unknown VLAN
  ----  ---------  + ------------   |  ----  ---------  + ------------
  1     10/100TX   | Learn          |  8     10/100TX   | Learn
  2     10/100TX   | Learn          |  9     10/100TX   | Learn
  3     10/100TX   | Learn          |  10    10/100TX   | Learn
  4     10/100TX   | Learn          |  11    10/100TX   | Learn
  5     10/100TX   | Learn          |  12    10/100TX   | Learn
  6     10/100TX   | Learn          |  13               | Learn
  7     10/100TX   | Learn          |  14               | Learn

 Actions->   Cancel     Edit      Save      Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure 9-61. Example Showing Default Settings for Handling Advertisements**

3. Use the arrow keys to select the port you want, and the Space bar to select Unknown VLAN option for any ports you want to change.
4. When you finish making configuration changes, press [Return], then [S] (for **Save**) to save your changes to the Startup-Config file.

## CLI: Viewing and Configuring GVRP

**GVRP Commands Used in This Section**

| | |
|---|---|
| show gvrp | below |
| gvrp | page 9-84 |
| unknown-vlans | page 9-84 |

**Displaying the Switch's Current GVRP Configuration.** This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see "Port-Based Virtual LANs (Static VLANs)" on page 9-48.)

***Syntax:*** show gvrp

```
SMC TigerSwitch 10/100(config)# show gvrp

 GVRP support

  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : No
```

**Figure 9-62. Example of "Show GVRP" Listing with GVRP Disabled**

```
SMC TigerSwitch 10/100(config)# show gvrp
 GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes

  Port Type       | Unknown VLAN
  ---- ---------- + ------------
  1    10/100TX   | Learn
  2    10/100TX   | Learn
  3    10/100TX   | Block
  4    10/100TX   | Disable
  5    10/100TX   | Disable
  6    10/100TX   | Learn
  7    10/100TX   | Learn
  .       .       |   .
  .       .       |   .
  .       .       |   .
```

This example includes non-default settings for the Unknown VLAN field for some ports.

**Figure 9-63. Example of Show GVRP Listing with GVRP Enabled**

**Enabling and Disabling GVRP on the Switch.** This command enables GVRP on the switch.

***Syntax:*** gvrp

This example enables GVRP:

```
SMC TigerSwitch 10/100(config)# gvrp
```

This example disables GVRP operation on the switch:

```
SMC TigerSwitch 10/100(config)# no gvrp
```

**Enabling and Disabling GVRP On Individual Ports.** When GVRP is enabled on the switch, use the **unknown-vlans** command to change the Unknown VLAN field for one or more ports. You can use this command at either the Manager level or the interface context level for the desired port(s).

| | | |
|---|---|---|
| ***Syntax:*** | show gvrp | Shows the current settings. |
| | interface <*port-list*> unknown-vlans <learn \| block \| disable> | Changes the Unknown VLAN field setting for the specified port(s). |

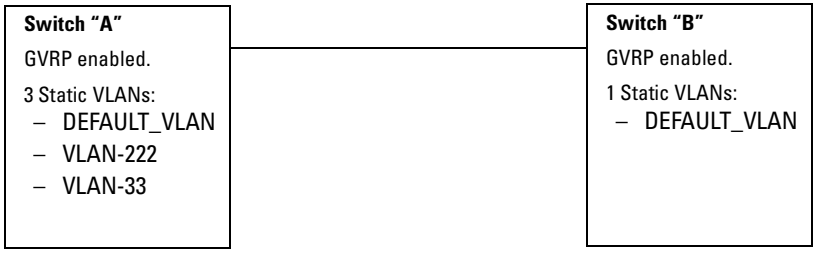
For example, to view and change the configuration for ports 1-2 to **Block**:

```
SMC TigerSwitch 10/100(config)# show gvrp
GVRP support
 Maximum VLANs to support : 8
 Primary VLAN : DEFAULT_VLAN
 GVRP Enabled : Yes
 Port Type      | Unknown VLAN
 ---- --------- + ------------
 1    10/100TX  | Learn
 2    10/100TX  | Learn
 .       .      |   .
 .       .      |   .
 .       .      |   .
SMC TigerSwitch 10/100(config)# interface 1-2 unknown-vlans
block
```

**Displaying the Static and Dynamic VLANs Active on the Switch.** The **show vlans** command lists all VLANs present in the switch.

***Syntax:*** show vlans

For example, in the following illustration, switch "A" has one static VLAN (the default VLAN), with GVRP enabled and port 1 configured to **Learn** for Unknown VLANs. Switch "B" has GVRP enabled and has three static VLANs: the default VLAN, VLAN-222, and VLAN-333. In this scenario, switch B will dynamically join VLAN-222 and VLAN-333:




The **show vlans** command lists the dynamic (and static) VLANs in switch "B".

```
Switch-B> show vlans
   Status and Counters - VLAN Information

    VLAN support : Yes
    Maximum VLANs to support : 8
    Primary VLAN : DEFAULT_VLAN

    802.1Q VLAN ID Name          Status
    -------------- ------------- ----------
    1              DEFAULT_VLAN  Static
    222            GVRP_222      Dynamic
    333            GVRP_333      Dynamic
```

Dynamic VLANs Learned from Switch "A" through Port 1

**Figure 9-64. Example of Listing Showing Dynamic VLANs**

**Converting a Dynamic VLAN to a Static VLAN.** If a port on the switch has joined a dynamic VLAN, you can use the following command to convert that dynamic VLAN to a static VLAN:

***Syntax:*** static <*dynamic-vlan-id*>

For example, to convert dynamic VLAN 333 (from the previous example) to a static VLAN:

```
SMC TigerSwitch 10/100(config)# static 333
```

### Web: Viewing and Configuring GVRP

To view, enable, disable, or reconfigure GVRP:

1. Click on the **Configuration** tab.
2. Click on [VLAN Configuration] and do the following:
   - To enable or disable GVRP, click on **GVRP Enabled**.
   - To change the Unknown VLAN field for any port:
     i. Click on [GVRP Security] and make the desired changes.
     ii. Click on [Apply] to save and implement your changes to the Unknown VLAN fields.

For web-based Help on how to use the web browser interface screen, click on the button provided on the web browser screen.

## GVRP Operating Notes

- A dynamic VLAN must be converted to a static VLAN before it can have an IP address.
- Converting a dynamic VLAN to a static VLAN and then executing the **write memory** command saves the VLAN in the startup-config file and makes it a permanent part of the switch's VLAN configuration.
- Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-ware will flood the GVRP (multicast) advertisement packets out all ports.
- GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, you must first convert it to a static VLAN.
- Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.

- By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices.
- A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.

# Multimedia Traffic Control with IP Multicast (IGMP)

**IGMP Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view igmp configuration | n/a | — | page 9-90 | — |
| show igmp status for multicast groups used by the selected VLAN | n/a | — | Yes | — |
| enabling or disabling IGMP (Requires VLAN ID Context) | disabled | — | page 9-92 | page 9-94 |
| per-port packet control | auto | — | page 9-93 | — |
| IGMP traffic priority | normal | — | page 9-93 | — |
| querier | enabled | — | page 9-94 | — |

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol controls). In the factory default state (IGMP disabled), the switch forwards all IGMP traffic to all ports, which can cause unnecessary bandwidth usage on ports not belonging to multicast groups. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. If no other querier is detected, the switch will then also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to "Changing the Querier Configuration Setting" on page 9-94.)

**Note**

IGMP configuration on the SMC6624M operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context. IGMP requires an IP address and subnet mask for any VLAN used for IGMP traffic. If the switch relies on DHCP or Bootp to acquire an IP address, ensure that an IP addressing has been assigned to the appropriate VLANs by using **show ip** or by viewing the menu interface "Management Address Information" screen (page 10-5).

In order for IGMP service to take effect, an IP address must be configured and active on the VLAN in which you want IGMP to operate. If the only VLAN on the switch is the default VLAN (VLAN ID, or VID, of "1"), then you must configure an IP address for VLAN 1. If multiple VLANs are configured, you must configure an IP address for the VLAN(s) in which you want to implement IGMP. Refer to "IP Configuration" on page 5-2.



## IGMP Operating Features

In the factory default configuration, IGMP is disabled. If multiple VLANs are not configured, you must configure IGMP on the default VLAN (DEFAULT_VLAN; VID = 1). If multiple VLANs are configured, you must configure IGMP on a per-VLAN basis. When you use either the CLI or the web browser interface to enable IGMP on the switch or a VLAN, the switch forwards IGMP traffic only to ports belonging to multicast groups. Using the console enables these additional options:

- **Forward with High Priority.** Disabling this parameter (the default) causes the switch or VLAN to process IP multicast traffic, along with other traffic, in the order received (normal priority). Enabling this parameter causes the switch or VLAN to give a higher priority to IP multicast traffic than to other traffic.
- **Auto/Blocked/Forward:** You can use the console to configure individual ports to any of the following states:
  - **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.

  - **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
  - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.

- **Querier:** In the default state (enabled), eliminates the need for a multicast router. In most cases, SMC recommends that you leave this parameter in the default "enabled" state even if you have a multicast router performing the querier function in your multicast group. For more information, see "How IGMP Operates" on page 9-94.

**Note**

Whenever IGMP is enabled, the switch generates an Event Log message indicating whether querier functionality is enabled.

For more information, refer to "How IGMP Operates" on page 9-94.

## CLI: Configuring and Displaying IGMP

**IGMP Commands Used in This Section**

| | |
|---|---|
| show ip igmp configuration | page 9-91 |
| ip igmp | page 9-92 |
| high-priority-forward | page 9-93 |
| auto <[ethernet] *<port-list>* | page 9-93 |
| blocked <[ethernet] *<port-list>* | page 9-93 |
| forward <[ethernet] *<port-list>* | page 9-93 |
| querier | page 9-94 |
| show ip igmp | See "IP Multicast (IGMP) Status" on page 10-16 |

**Viewing the Current IGMP Configuration.** This command lists the IGMP configuration for all VLANs configured on the switch or for a specific VLAN.

| | | |
|---|---|---|
| ***Syntax:*** | show ip igmp config | IGMP configuration for all VLANs on the switch |
| | show ip igmp *<vid>* config | IGMP configuration for a specific VLAN on the switch, including per-port data |

(For IGMP operating status, see "Internet Group Management Protocol (IGMP) Status" on page 10-16.)

For example, suppose you have the following VLAN and IGMP configurations on the switch:

| VLAN ID | VLAN Name | IGMP Enabled | Forward with High Priority | Querier |
|---|---|---|---|---|
| 1 | DEFAULT_VLAN | Yes | No | No |
| 22 | VLAN-2 | Yes | Yes | Yes |
| 33 | VLAN-3 | No | No | No |

You could use the CLI to display this data as follows:

```
SMC TigerSwitch 10/100> show ip igmp config
 IGMP Service
  VLAN ID      VLAN NAME    IGMP Enabled Forward with High Priority Querier
  ------------ ------------ ------------ -------------------------- -------
  1            DEFAULT_VLAN Yes          No                         No
  22           VLAN-2       Yes          Yes                        Yes
  33           VLAN-3       No           No                         Yes
```

**Figure 9-65. Example Listing of IGMP Configuration for All VLANs in the Switch**

The following version of the show ip igmp command includes the VLAN ID (*vid*) designation, and combines the above data with the IGMP per-port configuration:

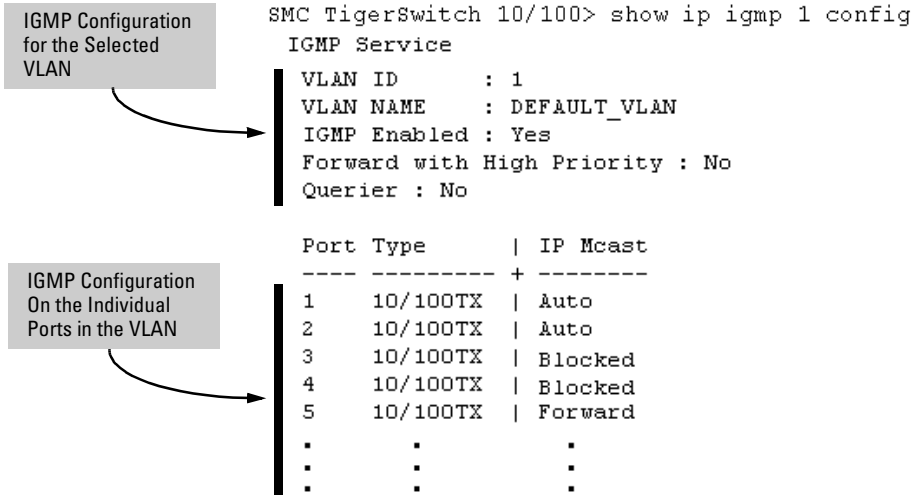



**Figure 9-66. Example Listing of IGMP Configuration for A Specific VLAN**

**Enabling or Disabling IGMP on a VLAN.** You can enable IGMP on a VLAN, along with the last-saved or default IGMP configuration (whichever was most recently set), or you can disable IGMP on a selected VLAN. Note that this command must be executed in a VLAN context.

***Syntax:*** [no] ip igmp

For example, here are methods to enable and disable IGMP on the default VLAN (VID = 1).

```
SMC TigerSwitch 10/100(config)# vlan 1 ip igmp
                                        Enables IGMP on VLAN 1.

SMC TigerSwitch 10/100(vlan-1)# ip igmp
                                        Same as above.

SMC TigerSwitch 10/100(config)# no vlan 1 ip igmp
                                        Disables IGMP on VLAN 1.
```

**Note**

If you disable IGMP on a VLAN and then later re-enable IGMP on that VLAN, the switch restores the last-saved IGMP configuration for that VLAN. For more on how switch memory operates, see appendic C, “Switch Memory and Configuration”.

You can also combine the **ip igmp** command with other IGMP-related commands, as described in the following sections.

**Configuring Per-Port IGMP Packet Control.** Use this command in the VLAN context to specify how each port should handle IGMP traffic.

***Syntax:*** vlan <*vid*> ip igmp
[auto <*port-list*> | blocked <*port-list*> | forward <*port-list*>]

***Default:*** auto

For example, suppose you wanted to configure IGMP as follows for VLAN 1 on the 10/100 ports on the SMC6624M:

| | | |
|---|---|---|
| Ports 1-7 | auto | Filter multicast traffic. Forward IGMP traffic to hosts on these ports that belong to the multicast group for which the traffic is intended. (Also forward any multicast traffic through any of these ports that is connected to a multicast router.) |
| Port 8 | forward | Forward all multicast traffic through this port. |
| Ports 9-12 | blocked | Drop all multicast traffic received from devices on these ports, and prevent any outgoing multicast traffic from moving through these ports. |

Depending on the privilege level, you could use one of the following commands to configure IGMP on VLAN 1 with the above settings:

```
SMC TigerSwitch 10/100(config)# vlan 1 ip igmp auto 1-7
forward 8 blocked 9-12
```

```
SMC TigerSwitch 10/100(vlan-1)# ip igmp auto 1-7 forward 8
blocked 9-12
```

The following command displays the VLAN and per-port configuration resulting from the above commands.

```
SMC TigerSwitch 10/100> show ip igmp 1 config
```

**Configuring IGMP Traffic Priority.** This command assigns "high" priority to IGMP traffic or returns a high-priority setting to "normal" priority.

***Syntax:*** `vlan <vid> ip igmp high-priority-forward`

***Default:*** normal

```
SMC TigerSwitch 10/100(config)# vlan 1 ip igmp high-
priority-forward
```
Configures high priority for IGMP traffic on VLAN 1.

```
SMC TigerSwitch 10/100(vlan-1)# vlan 1 ip igmp high-
priority-forward
```
Same as above command, but in the VLAN 1 context level.

```
SMC TigerSwitch 10/100(vlan 1)# no ip igmp high-priority-
forward
```

Returns IGMP traffic to “normal” priority.

```
SMC TigerSwitch 10/100> show ip igmp config
```

Show command to display results of above high-priority commands.

**Configuring the Querier Function.** The default querier function is “enabled”. This command disables or re-enables the querier function.

***Syntax:*** [no] vlan <*vid*> ip igmp querier

***Default:*** Yes

```
SMC TigerSwitch 10/100(config)# no vlan 1 ip igmp querier
```

Disables the querier function on VLAN 1.

```
SMC TigerSwitch 10/1002> show ip igmp config
```

Show command to display results of above querier command.

## Web: Enabling or Disabling IGMP

In the web browser interface you can enable or disable IGMP on a per-VLAN basis. To configure other IGMP features, telnet to the switch console and use the CLI.

To Enable or Disable IGMP

1. Click on the **Configuration** tab.
2. Click on [Device Features].
3. If more than one VLAN is configured, use the VLAN pull-down menu to select the VLAN on which you want to enable or disable IGMP.
4. Use the Multicast Filtering (IGMP) menu to enable or disable IGMP.
5. Click on [Apply Changes] to implement the configuration change.

## How IGMP Operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. (In Hewlett-Packard’s implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the **querier** feature enabled.) A set of hosts, routers, and/or switches that send or receive multicast data streams

to or from the same source(s) is termed a *multicast group*, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network. (If you need to disable the querier feature, you can do so through the CLI, using the IGMP configuration MIB. See "Changing the Querier Configuration Setting" on page "Configuring the Querier Function" on page 9-94.)
- **Report:** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

**IGMP Data.** To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see "IP Multicast (IGMP) Status" on page 10-16.

## Role of the Switch

When IGMP is enabled on the switch, it examines the IGMP packets it receives:

- To learn which of its ports are linked to IGMP hosts and multicast routers/queriers belonging to any multicast group
- To become a querier if a multicast router/querier is not discovered on the network

Once the switch learns the port location of the hosts belonging to any particular multicast group, it can direct group traffic to only those ports, resulting in bandwidth savings on ports where group members do not reside. The following example illustrates this operation.

Figure 9-67 on page 9-96 shows a network running IGMP.

- PCs 1 and 4, switch 2, and all of the routers are members of an IP multicast group. (The routers operate as queriers.)
- Switch 1 ignores IGMP traffic and does not distinguish between IP multicast group members and non-members. Thus, it is sending large amounts of unwanted multicast traffic out the ports to PCs 2 and 3.

- Switch 2 is recognizing IGMP traffic and learns that PC 4 is in the IP multicast group receiving multicast data from the video server (PC X). Switch 2 then sends the multicast data only to the port for PC 4, thus avoiding unwanted multicast traffic on the ports for PCs 5 and 6.

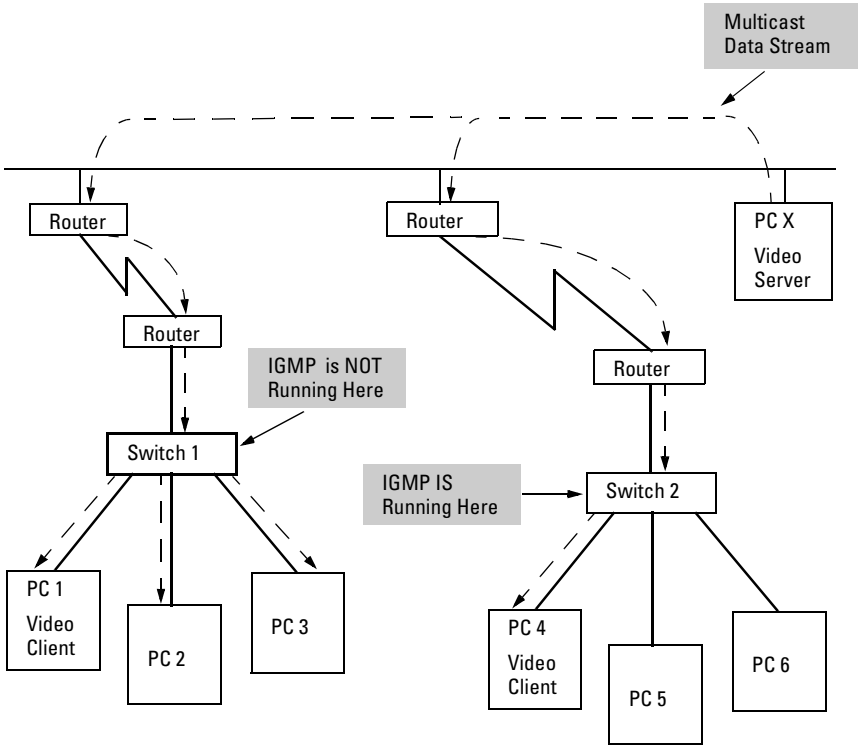



**Figure 9-67. The Advantage of Using IGMP**

The next figure (9-68) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier.

PCs 2, 5, and 6 are members of the same IP multicast group.

IGMP is configured on switches 3 and 4. Either of these switches can operate as querier because a multicast router is not present on the network. (If an IGMP switch does not detect a querier, it automatically assumes this role, assuming the querier feature is enabled—the default—within IGMP.)

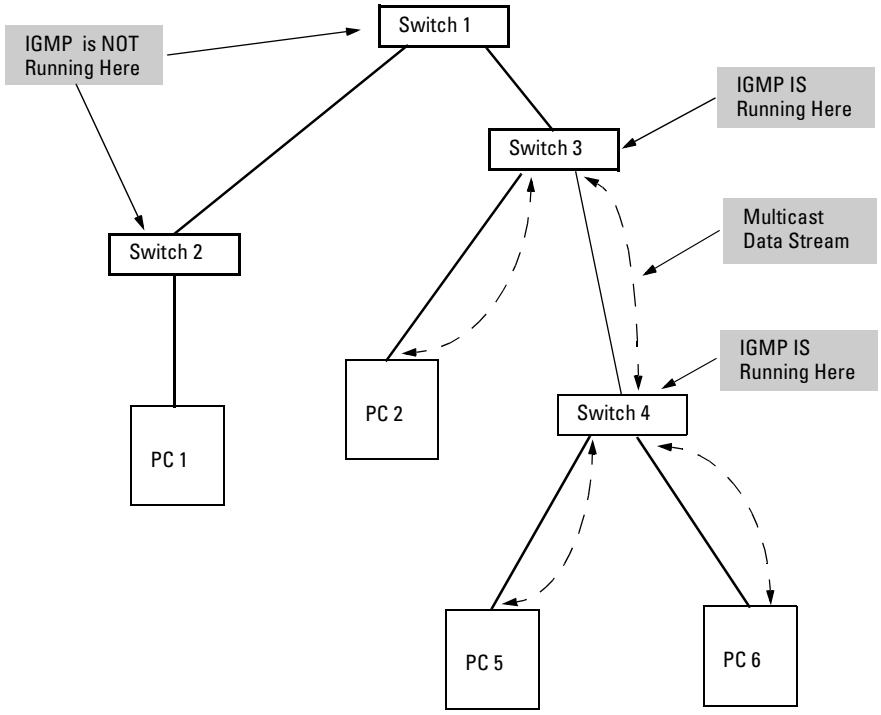



**Figure 9-68. Isolating IP Multicast Traffic in a Network**

- In the above figure, the multicast group traffic does not go to switch 1 and beyond because either the port on switch 3 that connects to switch 1 has been configured as blocked or there are no hosts connected to switch 1 or switch 2 that belong to the multicast group.
- For PC 1 to become a member of the same multicast group without flooding IP multicast traffic on all ports of switches 1 and 2, IGMP must be configured on both switches 1 and 2, and the port on Switch 3 that connects to Switch 1 must be unblocked.

**Note:**

**IP Multicast Filters.** IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Devices that have static Traffic/Security filters configured with a "Multicast" filter type and a "Multicast Address" in this range will continue in effect unless IGMP learns of a multicast group destination in this range. In that case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address formerly controlled by IGMP. (Note that the SMC6624M does not have traffic/security filters.)

**Reserved Addresses Excluded from IP Multicast (IGMP) Filtering.** Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are "well known" or "reserved" addresses. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

## Number of IP Multicast Addresses Allowed

Multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

# Spanning Tree Protocol (STP)

**STP Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing the STP configuration | n/a | page 9-100 | page 9-102 | — |
| enable/disable STP | disabled | page 9-100 | page 9-103 | page 9-105 |
| reconfiguring general operation | priority: 32768<br>max age: 20 s<br>hello time: 2 s<br>fwd. delay: 15 s | page 9-100 | page 9-103 | |
| reconfiguring per-port STP | path cost: var<br>priority: 128<br>mode: norm | page 9-100 | page 9-104 | |
| monitoring STP | n/a | page 10-14 | page 10-15 | n/a |

The switch uses the IEEE 802.1D Spanning Tree Protocol (STP), when enabled, to ensure that only one path at a time is active between any two nodes on the network. In networks where there is more than one physical path between any two nodes, STP ensures a single active path between them by blocking all redundant paths. Enabling STP is necessary in such networks because having more than one path between a pair of nodes causes loops in the network, which can result in duplication of messages, leading to a "broadcast storm" that can bring down the network.

**Note**

You should enable STP in any switch that is part of a redundant physical link (loop topology). (It is recommended that you enable STP on all switches belonging to a loop topology.) This topic is covered in more detail under "How STP Operates" on page 9-105.

As recommended in the IEEE 802.1Q VLAN standard, the SMC6624M uses **single-instance STP**; a single spanning tree is created to make sure there are no network loops associated with any of the connections to the switch, regardless of whether VLANs are configured on the switch. Thus, these switches do not distinguish between VLANs when identifying redundant physical links. If VLANs are configured on the switch, see "STP Operation with 802.1Q VLANs" on page 9-107.

**STP Fast Mode for Overcoming Server Access Failures.** If an end node is configured to automatically access a server, the duration of the STP startup sequence can result in a "server access failure". On ports where this is a problem, configuring STP Fast Mode can eliminate the failure. For more information, see "STP Fast Mode" on page 9-106. Also, for more information on STP, see "How STP Operates" on page 9-105.

In the factory default configuration, STP is off. If a redundant link (loop) exists between nodes in your network, you should enable Spanning Tree.

**Note**

STP retains its current parameter settings when disabled. Thus, if you disable STP, then later re-enable it, the parameter settings will be the same as before STP was disabled.

**Caution**

Because the switch automatically gives faster links a higher priority, the default STP parameter settings are usually adequate for spanning tree operation. Also because incorrect STP settings can adversely affect network performance, you should not make changes unless you have a strong understanding of how STP operates. For more on STP, see the IEEE 802.1D standard.

## Menu: Configuring STP

1. From the Main Menu, select:
   **2. Switch Configuration . . .**
   **4. Spanning Tree Operation**
2. Press [E] (for **Edit**) to highlight the **Spanning Tree Enabled** parameter.
3. Press the Space bar to select **Yes** . (This enables STP.

)

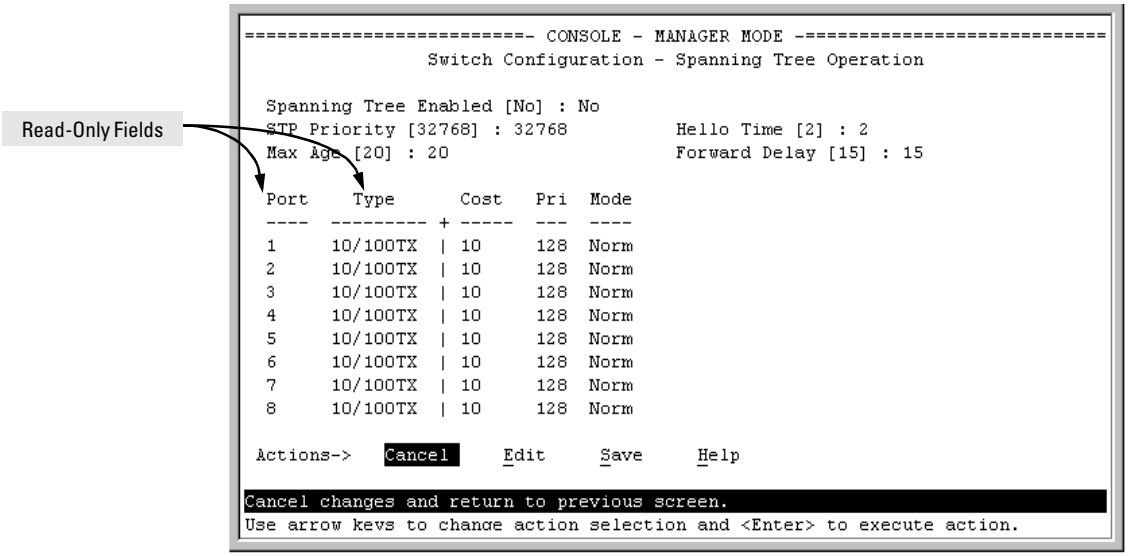



**Figure 9-69. Example of the STP Configuration Screen**

4. If the remaining STP parameter settings are adequate for your network, go to step 8.
5. Use [Tab] or the arrow keys to select the next parameter you want to change, then type in the new value or press the Space Bar to select a value. (If you need information on STP parameters, press [Enter] to select the **Actions** line, then press **H** to get help.)
6. Repeat step 5 for each additional parameter you want to change.

   *For information on the Mode parameter, see "STP Fast Mode" on page 9-106.*
7. When you are finished editing parameters, press [Enter] to return to the **Actions** line.
8. Press [S] to save the currently displayed STP parameter settings, then return to the Main Menu.

# CLI: Configuring STP

**STP Commands Used in This Section**

| | |
|---|---|
| show spanning-tree config | Below |
| spanning-tree | page 9-103 |
| forward-delay *<4 - 30>* | page 9-103 |
| hello-time *<1 - 10>* | page 9-103 |
| maximum-age *<6 - 40>* | page 9-103 |
| priority *<0 - 65535>* | page 9-103 |
| ethernet *<port-list>* | page 9-104 |
| path-cost *<1 - 65535>* | page 9-104 |
| priority *<0 - 255>* | page 9-104 |
| mode *<norm \| fast>* | page 9-104 |
| show spanning tree | See "Spanning Tree Protocol (STP) Information" on page 10-14 |

**Viewing the Current STP Configuration.** Regardless of whether STP is disabled (the default), this command lists the switch's full STP configuration, including general settings and port settings.

***Syntax:*** show spanning-tree configuration

Default: See figure 9-70, below.

In the default configuration, STP appears as shown here:

```
SMC TigerSwitch 10/100> show spanning-tree config
  Spanning Tree Operation
   Spanning Tree Enabled : No
   STP Priority : 32768                Hello Time : 2
   Max Age : 20                        Forward Delay : 15

   Port Type       | Cost   Pri Mode
   ---- ---------- + ------ --- ----
   1    10/100TX   | 10     128 Norm
   2    10/100TX   | 10     128 Norm
   3    10/100TX   | 10     128 Norm
   4    10/100TX   | 10     128 Norm
   5    10/100TX   | 10     128 Norm
   .       .         .      .   .
   .       .         .      .   .
   .       .         .      .   .
```

**Figure 9-70. Example of the Default STP Configuration Listing**

**Enabling or Disabling STP.** Enabling STP implements the spanning-tree protocol for all physical ports on the switch, regardless of whether multiple VLANs are configured. Disabling STP removes protection against redundant loops that can significantly slow or halt a network.

***Syntax:*** [no] spanning-tree
***Default:*** Disabled

This command enables STP with the current parameter settings or disables STP withoug losing the most-recently configured parameter settings. (To learn how the switch handles parameter changes, how to test changes without losing the previous settings, and how to replace previous settings with new settings, see appendix C, "Switch Memory and Configuration".) When enabling STP, you can also include the STP general and per-port parameters described in the next two sections. When you use the "no" form of the command, you can do so only to disable STP. (STP parameter settings are not changed when you disable STP, and cannot be included with the no spanning-tree command.

**Caution**

Because incorrect STP settings can adversely affect network performance, SMC recommends that you use the default STP parameter settings. You should not change these settings unless you have a strong understanding of how STP operates. For more on STP, see the IEEE 802.1D standard.

```
SMC TigerSwitch 10/100(config)# spanning tree
```
Enables STP on the switch.

**Reconfiguring General STP Operation on the Switch.** This command enables STP (if it is not already enabled) and configures one or more of the following parameters:

**Table 9-10.General STP Operating Parameters**

| Name | Default | Range | Function |
|---|---|---|---|
| priority | 32768 | 0 - 65535 | Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority. |
| maximum-age | 20 seconds | 6 - 40 seconds | Maximum received message age the switch allows for STP information before discarding the message, |
| hello-time | 2 seconds | 1 - 10 | Time between messages transmitted when the switch is the root. |
| forward-delay | 15 seconds | 4 - 30 seconds | Time the switch waits before transitioning from the listening to the learning state, and between the learning state to the forwarding state. |

You can also include one or more of the STP per-port parameters in this command. See "Reconfiguring Per-Port STP Operation on the Switch" on page 9-104.

***Syntax:*** spanning-tree
priority <0 - 65355>
maximum-age <6 - 40 seconds>
hello-time <1 - 10 seconds>
forward-delay <4 - 30 seconds>

***Default:*** See table 9-10, above.

For example, to enable STP with a maximum-age of 30 seconds and a hello-time of 3 seconds:

```
SMC TigerSwitch 10/100(config)# spanning tree maximum-age
30 hello-time 3
```

**Reconfiguring Per-Port STP Operation on the Switch.** This command enables STP (if not already enabled) and configures the following per-port parameters:

**Table 9-11.Per-Port STP Parameters**

| Name | Default | Range | Function |
|---|---|---|---|
| path-cost | Ethernet: 100<br>10/100Tx: 10<br>100 Fx: 10<br>Gigabit: 5 | 1 - 65535 | Assigns an individual port cost that the switch uses to determine which ports are the forwarding ports. |
| priority | 128 | 0 - 255 | Used by STP to determine the port(s) to use for forwarding. The port with the lowest number has the highest priority. |
| mode | norm | norm<br>*- or -*<br>fast | Specifies whether a port progresses through the listening, learning, and forwarding (or blocking) states ("norm" mode) or transitions directly to the forwarding state ("fast" mode).<br>*(For information on when to use Fast mode, see "STP Fast Mode" on page 9-106.)* |

You can also include STP general parameters in this command. See "Reconfiguring General STP Operation on the Switch" on page 9-103.

***Syntax:*** spanning-tree ethernet <*port-list*>
path-cost *<1 - 65535>*
priority *<0 - 255>*
mode *<norm | fast>*

***Default:*** See table 9-11, above.

For example, the following enables STP (if it is not already enabled) and configures ports 5 and 6 to a path cost of **15**, a priority of **100**, and **fast** mode:

```
SMC TigerSwitch 10/100(config)# spanning-tree ethernet 5-
6 path-cost 15 priority 100 mode fast
```

## Web: Enabling or Disabling STP

In the web browser interface you can enable or disable STP on the switch. To configure other STP features, telnet to the switch console and use the CLI.

To enable or disable STP on the switch:

1. Click on the **Configuration** tab
2. Click on [Device Features].
3. Enable or Disable STP by selecting On or Off from the pull-down menu.
4. Click on [Apply Changes] to implement the configuration change.

## How STP Operates

The switch automatically senses port identity and type, and automatically defines port cost and priority for each type. The console interface allows you to adjust the Cost and Priority for each port, as well as the Mode for each port and the global STP parameter values for the switch.

While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down. For example:

- Active path from node A to node B: 1—> 3
- Backup (redundant) path from node A to node B: 4 —> 2 —> 3

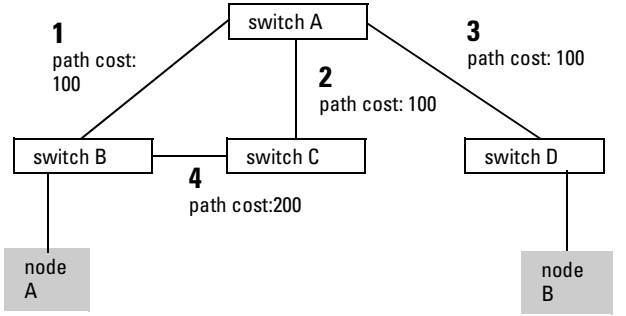



**Figure 9-71. Example of Redundant Paths Between Two Nodes**

## STP Fast Mode

For standard STP operation, when a network connection is established on a device that is running STP, the port used for the connection goes through a sequence of states (Listening and Learning) before getting to its final state (Forwarding or Blocking, as determined by the STP negotiation). This sequence takes two times the forward delay value configured for the switch. The default is 15 seconds on SMC switches, per the IEEE 802.1D standard recommendation, resulting in a total STP negotiation time of 30 seconds. Each switch port goes through this start-up sequence whenever the network connection is established on the port. This includes, for example, when the switch or connected device is powered up, or the network cable is connected.

A problem can arise from this long STP start-up sequence because some end nodes are configured to automatically try to access a network server whenever the end node detects a network connection. Typical server access includes to Novell servers, DHCP servers, and X terminal servers. If the server access is attempted during the time that the switch port is negotiating its STP state, the server access will fail. To provide support for this end node behavior, the SMC6624M offers a configuration mode, called “Fast Mode”, that causes the switch port to skip the standard STP start-up sequence and put the port directly into the “Forwarding” state, thus allowing the server access request to be forwarded when the end node needs it.

If you encounter end nodes that repeatedly indicate server access failure when attempting to bring up their network connection, and you have enabled STP on the switch, try changing the configuration of the switch ports associated with those end nodes to STP Fast Mode.

**Caution**

The Fast Mode configuration should be used only on switch ports connected to end nodes. Changing the Mode to Fast on ports connected to hubs, switches, or routers may cause loops in your network that STP may not be able to immediately detect, in all cases. This will cause temporary loops in your network. After the fast start-up sequence, though, the switch ports operate according to the STP standard, and will adjust their state to eliminate continuing network loops.



**To Configure Fast Mode for a Switch Port:**

- In the CLI, use this command: spanning tree mode *<port list>* fast

  For example, to configure Fast mode for ports 1-3 and 5:

  ```
  SMC TigerSwitch 10/100(config)# spanning-tree ethernet
  1-3,5 mode fast
  ```

- In the menu interface, go to the Main Menu and follow the steps under "Menu: Configuring STP" on page 9-100.

## STP Operation with 802.1Q VLANs

As recommended in the IEEE 802.1Q VLAN standard, when spanning tree is enabled on the switch, a single spanning tree is configured for all ports across the switch, including those in separate VLANs. This means that if redundant physical links exist in separate VLANs, spanning tree will block all but one of those links. However, if you need to use STP on the SMC6624M in a VLAN environment with redundant physical links, you can prevent blocked redundant links by using a port trunk. The following example shows how you can use a port trunk with 802.1Q (tagged) VLANs and STP without unnecessarily blocking any links or losing any bandwidth.

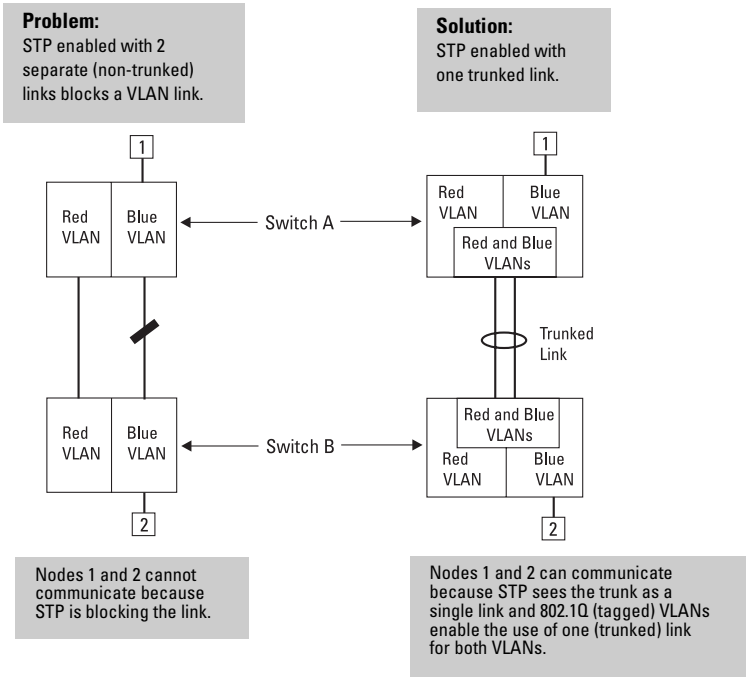



**Figure 9-72. Example of Using a Trunked Link with STP and VLANs**

For more information, refer to "Spanning Tree Protocol Operation with VLANs" on page 9-71.

# Monitoring and Analyzing Switch Operation



The SMC6624M switch has several built-in tools for monitoring, analyzing, and troubleshooting switch and network operation:

- **Status:** Includes options for displaying general switch information, management address data, port status, MAC addresses detected on each port, and STP, IGMP, and VLAN data.
- **Counters:** Display details of traffic volume on individual ports.
- **Event Log**: Lists switch operating events.
- **Alert Log:** Lists network occurrences detected by the switch (in the Status | Overview screen of the web browser interface).
- **Configurable trap receivers:** Uses SNMP to enable management stations on your network to receive SNMP traps from the switch.
- **Port or VLAN monitoring (mirroring):** Copy all traffic from the specified ports or VLAN to a designated monitoring port.

**Note**

Link test, ping test, browse configuration, and the Command prompt—analysis tools in troubleshooting situations—are described in chapter 11, “Troubleshooting”. See “Diagnostic Tools” on page 13.

# Status and Counters Data

This section describes the status and counters screens available through the switch console interface and/or the web browser interface.

**Note** You can access all console screens from the web browser interface via Telnet to the console. Telnet access to the switch is available in the Device View window under the **Configuration** tab.



| Status or Counters Type | Interface | Purpose | Page |
|---|---|---|---|
| Menu Access to Status and Counters | Menu | Access menu interface for status and counter data. | **10-3** |
| General System Information | Menu, CLI | Lists switch-level operating information. | **10-4** |
| Management Address Information | Menu, CLI | Lists the MAC address, IP address, and IPX network number for each VLAN or, if no VLANs are configured, for the switch. | **10-5** |
| Port Status | Menu, CLI, Web | Displays the operational status of each port. | **10-6** |
| Port and Trunk Statistics | Menu, CLI, Web | Summarizes port activity. | **10-7** |
| Address Table (Address Forwarding Table) | Menu, CLI | Lists the MAC addresses of nodes the switch has detected on the network, with the corresponding switch port. | **10-10** |
| Port Address Table | Menu, CLI | Lists the MAC addresses that the switch has learned from the selected port. | **10-10** |
| STP Information | Menu, CLI | Lists Spanning Tree Protocol data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis. | **10-14** |
| IGMP Status | Menu, CLI | Lists IGMP groups, reports, queries, and port on which querier is located. | **10-16** |
| VLAN Information | Menu, CLI | For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status. | **10-17** |
| Port Status Overview | Web | Shows port utilization and the Alert Log. | **10-19** |

# Menu Access To Status and Counters

Beginning at the Main Menu, display the Status and Counters menu by selecting:

**1. Status and Counters**

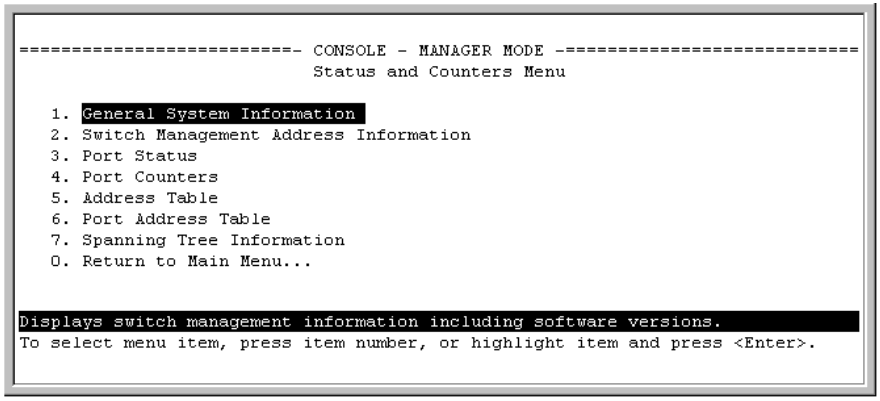



**Figure 10-1. The Status and Counters Menu**

Each of the above menu items accesses the read-only screens described on the following pages. Refer to the online help for a description of the entries displayed in these screens.

# General System Information

## Menu Access

From the console Main Menu, select:

**1. Status and Counters**

**1. General System Information**

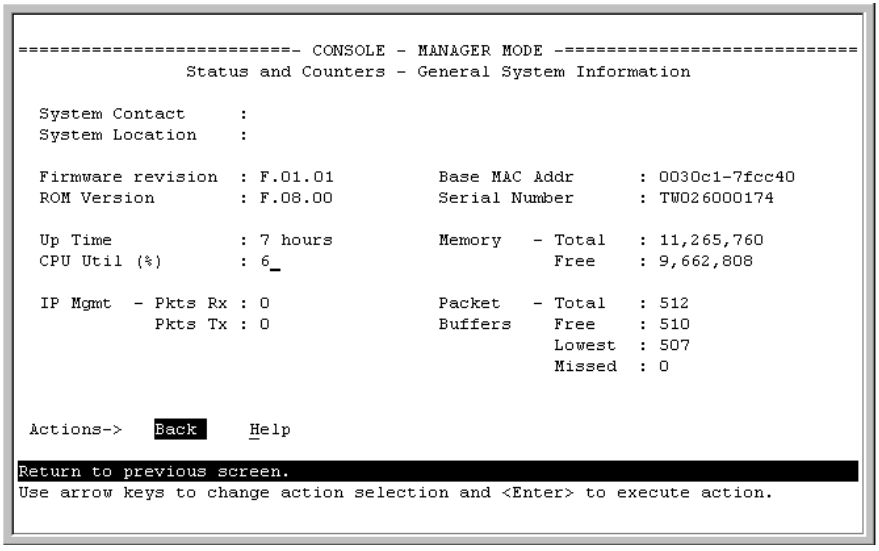



**Figure 10-2. Example of General Switch Information**

This screen dynamically indicates how individual switch resources are being used.

## CLI Access

***Syntax:*** show system-information

# Switch Management Address Information

## Menu Access

From the Main Menu, select:

**1 Status and Counters . . .**

**2. Switch Management Address Information**

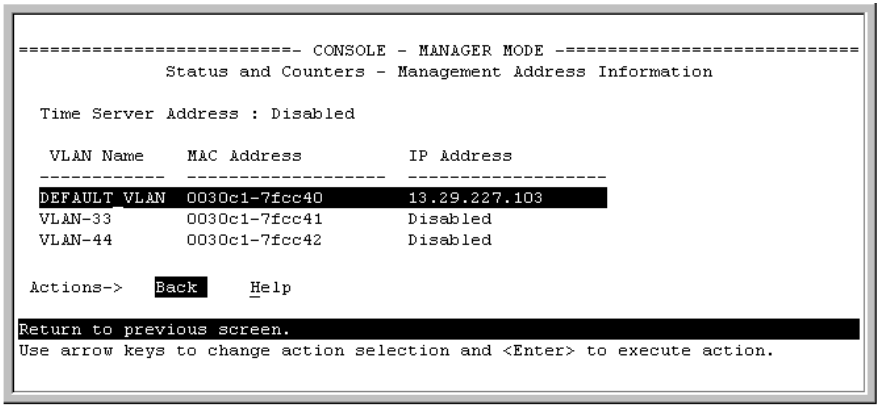



**Figure 10-3. Example of Management Address Information with VLANs Configured**

This screen displays addresses that are important for management of the switch. If multiple VLANs are *not* configured, this screen displays a single IP address for the entire switch.

## CLI Access

***Syntax:*** show management

# Port Status

The web browser interface and the console interface show the same port status data.

## Menu: Displaying Port Status

From the Main Menu, select:

**1. Status and Counters . . .3. Port Status**

```
=========================- CONSOLE - MANAGER MODE -============================
                      Status and Counters - Port Status

                   Intrusion                                  Flow     Bcast
  Port    Type       Alert    Enabled  Status     Mode        Ctrl     Limit
  ----  ---------  ---------  -------  ------  ----------  ---------  ------
  1     10/100TX   No         Yes      Up      100FDx      off        0
  2     10/100TX   No         Yes      Down    10HDx       off        0
  3     10/100TX   No         Yes      Down    10HDx       off        0
  4     10/100TX   No         Yes      Down    10HDx       off        0
  5     10/100TX   No         Yes      Down    10HDx       off        0
  6     10/100TX   No         Yes      Down    10HDx       off        0
  7     10/100TX   No         Yes      Down    10HDx       off        0
  8     10/100TX   No         Yes      Down    10HDx       off        0
  9     10/100TX   No         Yes      Down    10HDx       off        0
  10    10/100TX   No         Yes      Down    10HDx       off        0
  11    10/100TX   No         Yes      Down    10HDx       off        0

 Actions->   Back     Intrusion log     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 10-4. Example of Port Status on the Menu Interface**

## CLI Access

***Syntax:*** show interfaces

## Web Access

1. Click on the **Status** tab.
2. Click on [Port Status].

# Viewing Port and Trunk Group Statistics

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port and trunk statistics for all ports | n/a | page 10-8 | page 10-9 | page 10-9 |
| viewing a detailed summary for a particular port or trunk | n/a | page 10-8 | page 10-9 | page 10-9 |
| resetting counters | n/a | page 10-8 | page 10-9 | page 10-9 |

These features enable you to determine the traffic patterns for each port since the last reboot or reset of the switch. You can display:

- A general report of traffic on all LAN ports and trunk groups in the switch
- A detailed summary of traffic on a selected port or trunk group.

You can also reset the counters for a specific port.

The menu interface and the web browser interface provide a dynamic display of counters summarizing the traffic on each port. The CLI lets you see a static "snapshot" of port or trunk group statistics at a particular moment.

As mentioned above, rebooting or resetting the switch resets the counters to zero. You can also reset the counters to zero for the current session. This is useful for troubleshooting. See the "Note On Reset", below.

**Note on Reset**

The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Thus, using the **Reset** action resets the displayed counters to zero for the current session only. Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

## Menu Access to Port and Trunk Statistics

To access this screen from the Main Menu, select:

1. **Status and Counters . . .**
   4. **Port Counters**

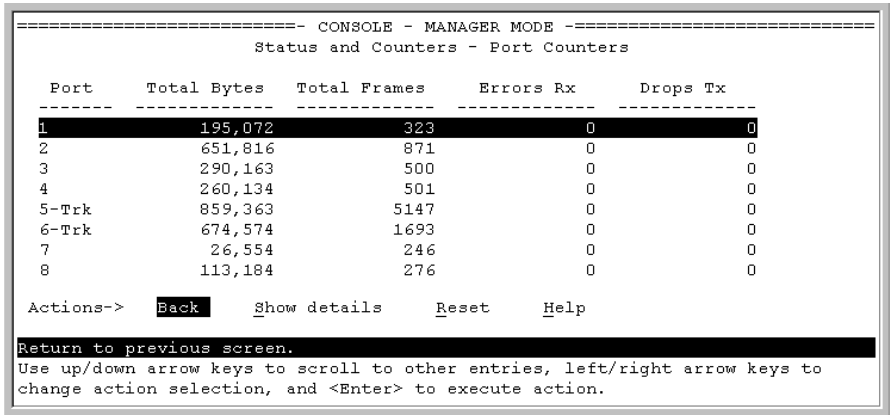



**Figure 10-5. Example of Port Counters on the Menu Interface**

To view details about the traffic on a particular port, use the ↓ key to highlight that port number, then select **Show Details**. For example, selecting port 2 displays a screen similar to figure 10-6, below.

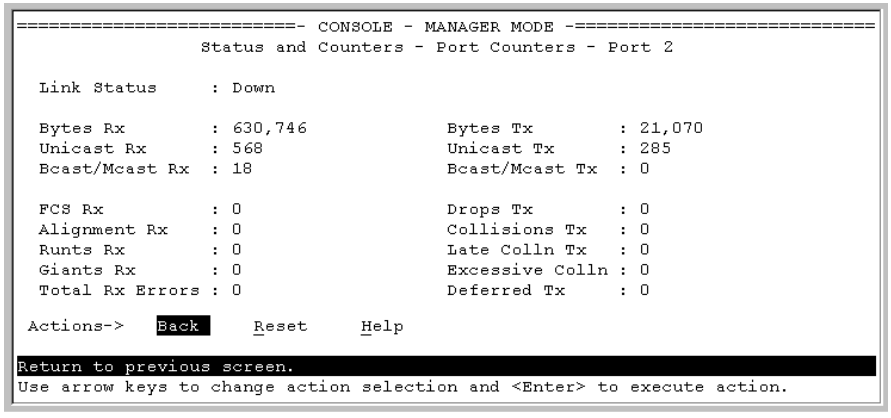



**Figure 10-6. Example of the Display for Show details on a Selected Port**

This screen also includes the **Reset** action for the current session. (See the “Note on Reset” on page 10-7.)

## CLI Access To Port and Trunk Group Statistics

**To Display the Port Counter Summary Report.** This command provides an overview of port activity for all ports on the switch.

***Syntax:*** show statistics

**To Display a Detailed Traffic Summary for a Specific Port.** This command provides traffic details for the port you specify.

***Syntax:*** show statistics *<port-number>*

**To Reset the Port Counters for a Specific Port.** This command resets the counters for the specified ports to zero for the current session. (See the "Note on Reset" on page 10-7.)

***Syntax:*** clear statistics <[ethernet] *port-list*>

## Web Browser Access To View Port and Trunk Group Statistics

1. Click on the **Status** tab.
2. Click on [Port Counters].
3. To reset the counters for a specific port, click anywhere in the row for that port, then click on [Refresh].

# Viewing the Switch's MAC Address Tables

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing MAC addresses on all ports | n/a | page 10-11 | page 10-13 | — |
| viewing MAC addresses on a specific port | n/a | page 10-12 | page 10-13 | — |
| viewing MAC addresses on a specific VLAN | n/a | — | page 10-13 | — |
| searching for a MAC address | n/a | page 10-12 | page 10-13 | — |



These features help you to view:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

## Menu Access to the MAC Address Views and Searches

**Switch-Level MAC-Address Viewing and Searching.** This feature lets you determine which switch port is being used to communicate with a specific device on the network. The listing includes:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

From the Main Menu, select:

**1. Status and Counters**
**5. Address Table**

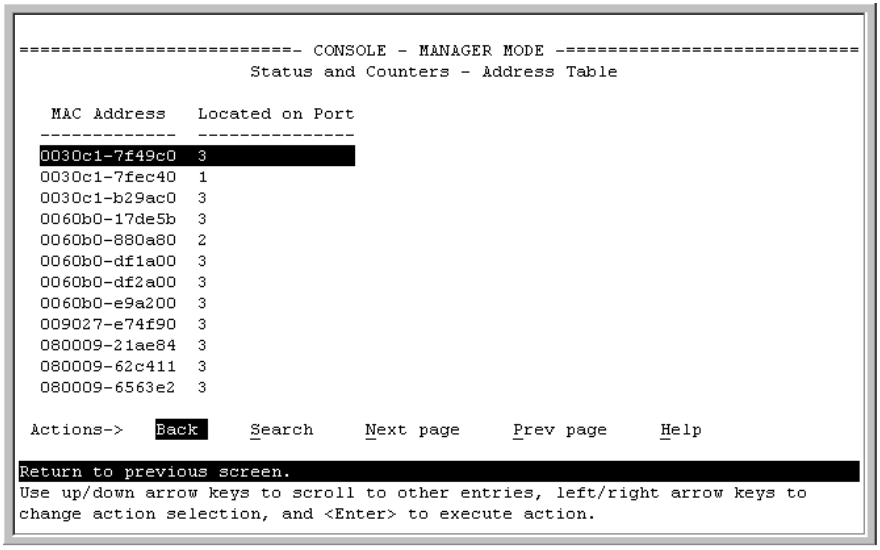



**Figure 10-7. Example of the Address Table**

To page through the listing, use **Next page** and **Prev page**.

**Identifying the Port Connection for a Specific Device.** This feature uses a device's MAC address that you enter to identify the port used by that device.

1. Proceeding from Figure 10-7, press [S] (for **Search**), to display the following prompt:

   ```
   Enter MAC address: _
   ```

2. Type the MAC address you want to locate and press [Enter]. The address and port number are highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.

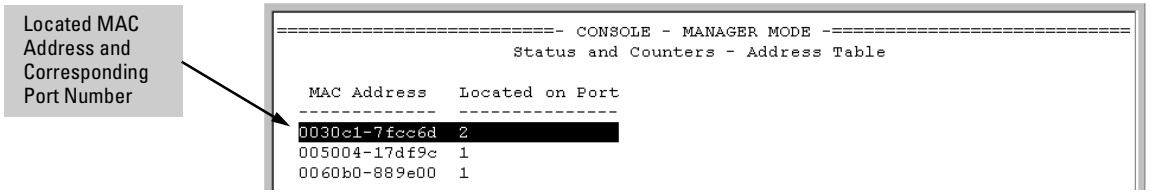



**Figure 10-8. Example of Menu Indicating Located MAC Address**

**Port-Level MAC Address Viewing and Searching.** This feature displays and searches for MAC addresses on the specified port instead of for all ports on the switch.

1. From the Main Menu, select:

   **1. Status and Counters**
   **6. Port Address Table**

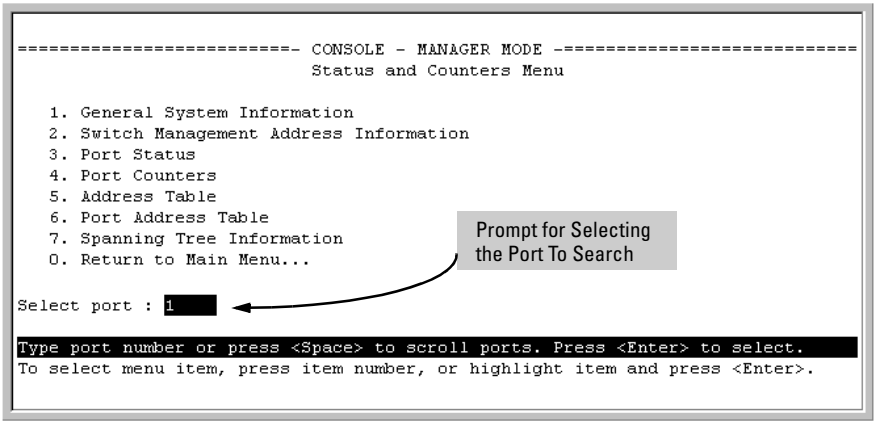



**Figure 10-9. Listing MAC Addresses for a Specific Port**

2. Use the Space bar to select the port you want to list or search for MAC addresses, then press [Enter] to list the MAC addresses detected on that port.

**Determining Whether a Specific Device Is Connected to the Selected Port.** Proceeding from step 2, above:

1. Press [S] (for **Search**), to display the following prompt:

```
Enter MAC address: _
```

2. Type the MAC address you want to locate and press [Enter]. The address is highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.

## CLI Access for MAC Address Views and Searches

***Syntax:*** show mac-address
[vlan <*vlan-id*>]
[ethernet]<*port-list*>]
[<mac-addr>]

**To List All Learned MAC Addresses on the Switch, with The Port Number on Which Each MAC Address Was Learned.**

```
SMC TigerSwitch 10/100> show mac-address
```

**To List All Learned MAC Addresses on one or more ports, with Their Corresponding Port Numbers.** For example, to list the learned MAC address on ports 1 through 5 and port 7:

```
SMC TigerSwitch 10/100> show mac-address 1-5,7
```

**To List All Learned MAC Addresses on a VLAN, with Their Port Numbers.** This command lists the MAC addresses associated with the ports for a given VLAN. For example:

```
SMC TigerSwitch 10/100> show mac-address vlan 100
```

**Note**

The SMC6624M switch has a Single Forwarding Database architecture. This means the switch has only a single MAC address table, and not a separate MAC address table per VLAN.

**To Find the Port On Which the Switch Learned a Specific MAC Address.** For example, to find the port on which the switch learns a MAC address of 0060b0-889e00:

```
SMC TigerSwitch 10/100> show mac-address 0060b0-889e00
```

# Spanning Tree Protocol (STP) Information

## Menu Access to STP Data

From the Main Menu, select:

**1. Status and Counters . . .**
**7. Spanning Tree Information**

STP must be enabled on the switch to display the following data:

```
============================- CONSOLE - MANAGER MODE -============================
                Status and Counters - Spanning Tree Information

  STP Enabled             : Yes
  Switch Priority         : 32,768
  Hello Time              : 2
  Max Age                 : 20
  Forward Delay           : 15

  Topology Change Count   : 3
  Time Since Last Change  : 4 mins

  Root MAC Address        : 0030c1-7fcc40
  Root Path Cost          : 0
  Root Port               : This switch is root
  Root Priority           : 32768


 Actions->    Back     Show ports     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure 10-10.Example of Spanning Tree Information**

Use this screen to determine current switch-level STP parameter settings and statistics.

You can use the **Show ports** action at the bottom of the screen to display port-level information and parameter settings for each port in the switch (including port type, cost, priority, operating state, and designated bridge) as shown in Figure 10-11.

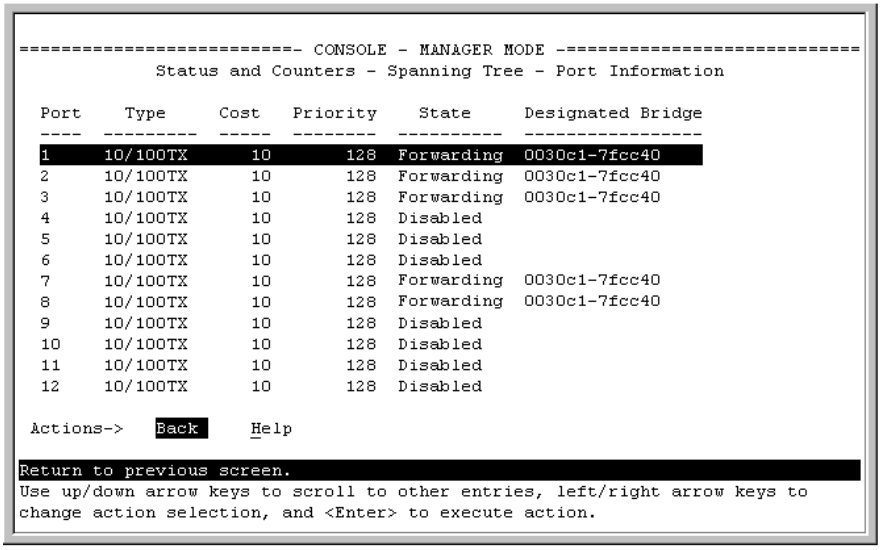



**Figure 10-11.Example of STP Port Information**

## CLI Access to STP Data

This option lists the STP configuration, root data, and per-port data (cost, priority, state, and designated bridge).

***Syntax:*** show spanning-tree

```
SMC TigerSwitch 10/100> show spanning-tree
```

## Internet Group Management Protocol (IGMP) Status

The switch uses the CLI to display the following IGMP status on a per-VLAN basis:

| Show Command | Output |
|---|---|
| show ip igmp | Global command listing IGMP status for all VLANs configured in the switch:<br>• VLAN ID (VID) and name<br>• Active group addresses per VLAN<br>• Number of report and query packets per group<br>• Querier access port per VLAN |
| show ip igmp <*vlan-id*> | Per-VLAN command listing above IGMP status for specified VLAN (VID) |
| show ip igmp group <*ip-addr*> | Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data. |

For example, suppose that **show ip igmp** listed an IGMP group address of 224.0.1.22. You could get additional data on that group by executing the following:

```
SMC TigerSwitch 10/100> show ip igmp group 224.0.1.22

 IGMP ports for group 224.0.1.22

  Port Type       Access       Age Timer Leave Timer
  ---- ---------- ------------ --------- -----------
  3    10/100TX   host         0         0
```

**Figure 10-12.Example of IGMP Group Data**

# VLAN Information

The switch uses the CLI to display the following VLAN status:

| Show Command | Output |
|---|---|
| show vlan | Lists:<br>• Maximum number of VLANs to support<br>• Existing VLANs<br>• Status (static or dynamic)<br>• Primary VLAN |
| show vlan <*vlan-id*> | For the specified VLAN, lists:<br>• Name, VID, and status (static/dynamic)<br>• Per-Port mode (tagged, untagged, forbid, no/auto)<br>• "Unknown VLAN" setting (Learn, Block, Disable)<br>• Port status (up/down) |

For example, suppose that your switch has the following VLANs:

| Ports | VLAN | VID |
|---|---|---|
| 1 - 12 | DEFAULT_VLAN | 1 |
| 1, 2 | VLAN-33 | 33 |
| 3, 4 | VLAN-44 | 44 |

The next three figures show how you could list data on the above VLANs.

**Listing the VLAN ID (VID) and Status for ALL VLANs in the Switch.**

```
SMC TigerSwitch 10/100> show vlan
  Status and Counters - VLAN Information
   VLAN support : Yes
   Maximum VLANs to support : 9
   Primary VLAN: DEFAULT_VLAN
   802.1Q VLAN ID Name          Status
   -------------- ------------- --------
   1              DEFAULT_VLAN  Static
   33             VLAN-33       Static
   44             VLAN-44       Static
```

**Figure 10-13.Example of VLAN Listing for the Entire Switch**

### Listing the VLAN ID (VID) and Status for Specific Ports.

Because ports 1 and 2 are not members of VLAN-44, it does not appear in this listing.

```
HP2512> show vlan ports 1-2
 Status and Counters - VLAN Information - for ports 1,2
  802.1Q VLAN ID Name          Status
  -------------- ------------- -------------
  1              DEFAULT_VLAN  Static
  33             VLAN-33       Static
```

**Figure 10-14.Example of VLAN Listing for Specific Ports**

### Listing Individual VLAN Status.

```
SMC TigerSwitch 10/100> show vlan ports 1-2
 Status and Counters - VLAN Information - Ports - VLAN 1
  802.1Q VLAN ID : 1
  Name           : DEFAULT_VLAN
  Status         : Static

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  1                Untagged Learn        Up
  2                Tagged   Learn        Up
  3                Untagged Learn        Up
  4                Untagged Learn        Down
  5                Untagged Learn        Down
  .                   .       .           .
  .                   .       .           .
  .                   .       .           .
```

# Web Browser Interface Status Information

The “home” screen for the web browser interface is the Status Overview screen, as shown below. As the title implies, it provides an overview of the status of the switch, including summary graphs indicating the network utilization on each of the switch ports, symbolic port status indicators, and the Alert Log, which informs you of any problems that may have occurred on the switch.

For more information on this screen, see chapter 4, “Using the Web Browser Interface”.

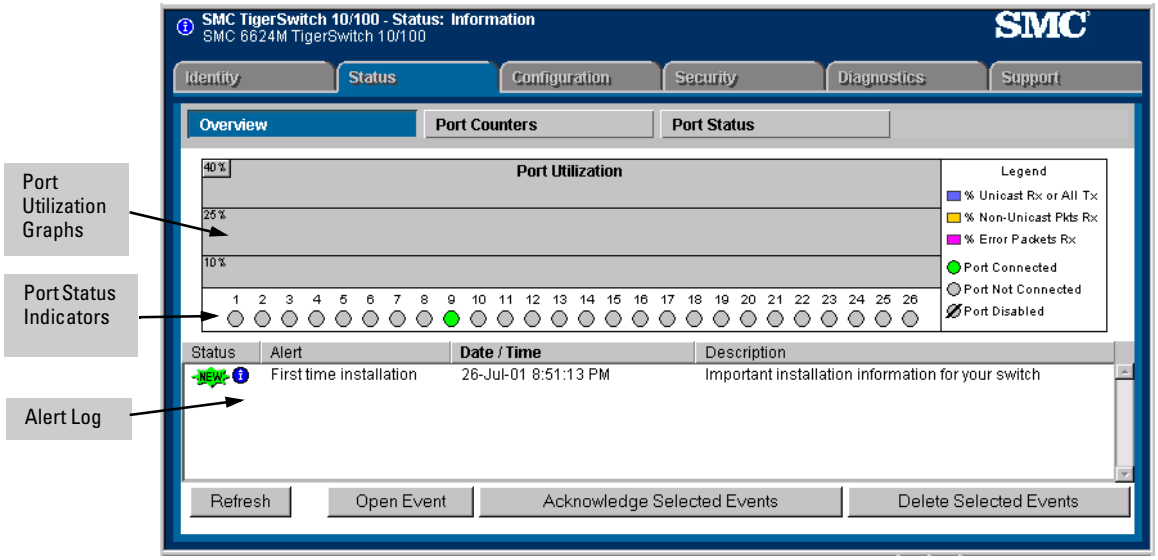



**Figure 10-15.Example of a Web Browser Interface Status Overview Screen**

# Port Monitoring Features

**Port Monitoring Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| display monitoring configuration | disabled | page 10-21 | page 10-23 | page 10-25 |
| configure the monitor port(s) or VLAN | ports: none<br>VLANs: DEFAULT_VLAN | page 10-21 | page 10-24 | page 10-25 |
| selecting or removing ports or VLANs | none selected | page 10-21 | page 10-24 | page 10-25 |



You can designate a port for monitoring traffic of one or more other ports or of a single VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources (ports or VLAN) to the designated monitoring port, to which a network analyzer can be attached.

**Note**

Port trunk groups cannot be used as a monitoring port.

It is possible, when monitoring multiple ports in networks with high traffic levels, to copy more traffic to a monitor port than the link can support. In this case, some packets may not be copied to the monitor port.

# Menu: Configuring Port Monitoring

This procedure describes configuring the switch for monitoring when monitoring is disabled. (If monitoring has already been enabled, the screens will appear differently than shown in this procedure.)

1. From the Console Main Menu, Select:

   **2. Switch Configuration...**

   **3. Network Monitoring Port**

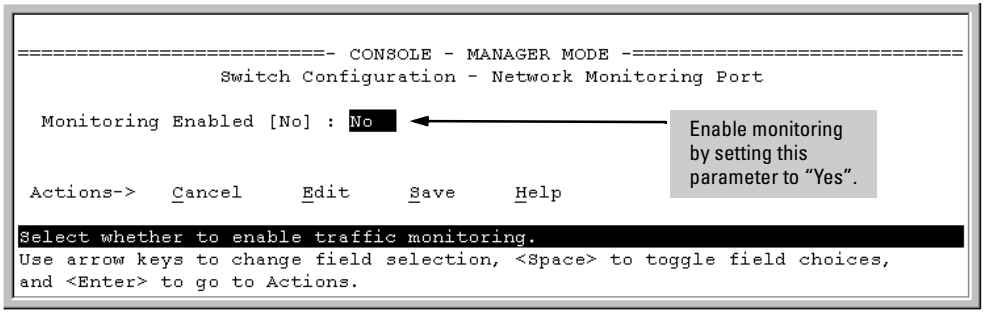



**Figure 10-16. The Default Network Monitoring Configuration Screen**

2. In the Actions menu, press [E] (for `Edit`).
3. If monitoring is currently disabled (the default) then enable it by pressing the Space bar (or [Y]) to select `Yes`.
4. Press the downarrow key to display a screen similar to the following and move the cursor to the **Monitoring Port** parameter.

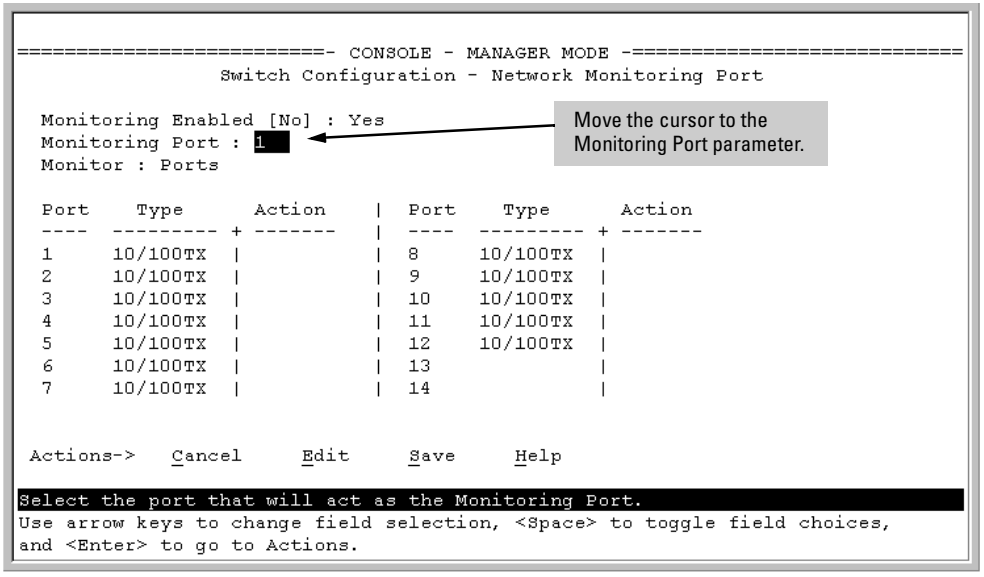



**Figure 10-17. How To Select a Monitoring Port**

5. Use the Space bar to select the port to use for monitoring, then press the downarrow key to select the **Monitor** parameter. (The default setting is **Ports**, which you will use if you want to monitor one or more individual ports on the switch.)

6. Do one of the following:
   - **To monitor individual ports:**
     i. Leave the **Monitor** parameter set to **Ports** and press the downarrow key to move the cursor to the **Action** column for the individual ports.
     ii. Press the Space bar to select **Monitor** for each port that you want monitored. (Use the downarrow key to move from one port to the next in the **Action** column.)
     iii. Press [Enter], then press [S] (for **Save**) to save your changes and exit from the screen.
   - **To monitor all ports in a VLAN:**
     i. Press the Space bar to select **VLAN** in the **Monitor** parameter,.
     ii. Press the downarrow keyto move to the **VLAN** parameter (Figure 10-18 on page page 10-23).
     iii. Press the Space bar again to select the VLAN that you want to monitor.

iv. Press [Enter], then press [S] (for `Save`) to save your changes and exit from the screen.

**Note:** This screen appears instead of the one in figure 10-17 if the Monitor parameter is set to VLAN

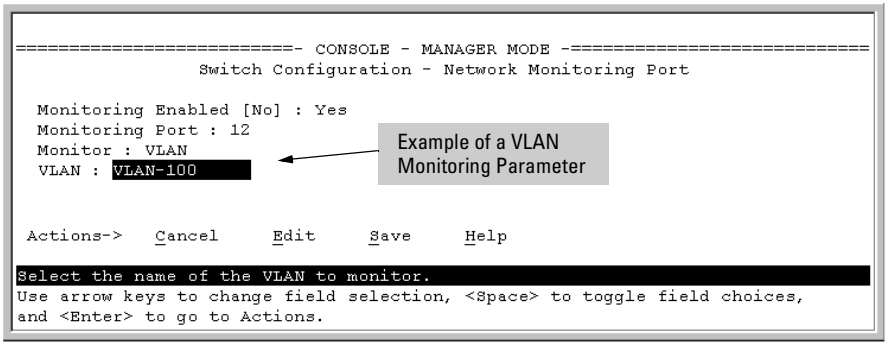



**Figure 10-18.Example of Selecting a VLAN to Monitor**

7. Return to the Main Menu.

# CLI: Configuring Port Monitoring

**Port Monitoring Commands Used in This Section**

| | |
|---|---|
| show mirror-port | below |
| mirror-port | page 10-24 |
| monitor (VLAN) | page 10-24 |
| monitor (Port) | page 10-24 |

You must use the following configuration sequence to configure port monitoring in the CLI:

1. Assign a monitoring (mirror) port.
2. Designate the port(s) and/or a VLAN to monitor.

**Displaying the Port Monitoring Configuration.** This command lists the port assigned to receive monitored traffic and the ports being monitored.

***Syntax:*** show mirror-port

For example, if you assign port 12 as the monitoring port and configure the switch to monitor ports 1 - 3, show mirror-port displays the following:

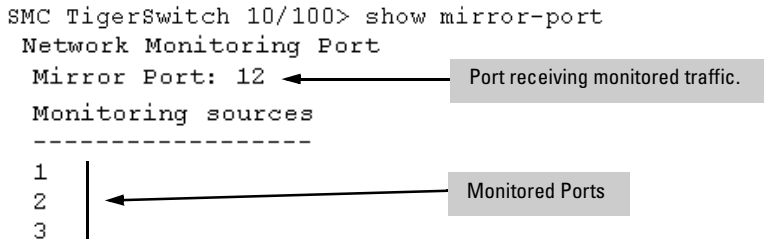



**Figure 10-19.Example of Monitored Port Listing**



**Configuring the Monitor Port.** This command assigns or removes a monitoring port, and must be executed from the global configuration level. Removing the monitor port disables port monitoring and resets the monitoring parameters to their factory-default settings.

***Syntax:*** [no] mirror-port [<*port-num*>]

For example, to assign port 12 as the monitoring port:

```
SMC TigerSwitch 10/100(config)# mirror-port 12
```

To turn off port monitoring:

```
SMC TigerSwitch 10/100(config)# no mirror-port
```

**Selecting or Removing Ports or VLANs As Monitoring Sources.** After you configure a monitor port you can use either the global configuration level or the interface context level to select ports or VLANs as monitoring sources. You can also use either level to remove monitoring sources.

***Syntax:*** [no] monitor [vlan <vlan-id> | interface ethernet <port-list>]

For example, with a monitoring (mirror) port configured (above), you could select ports 1 and 2 for monitoring:

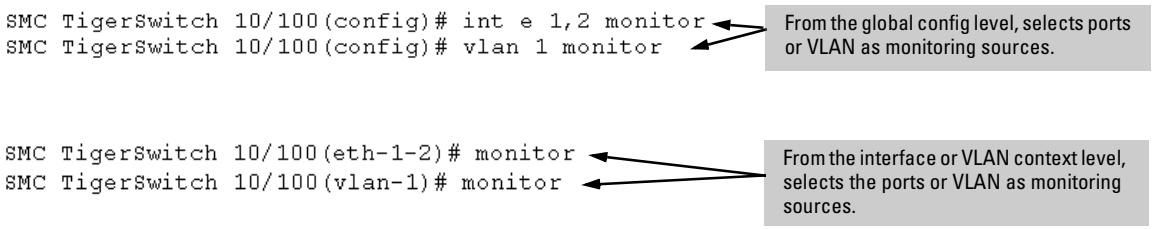



**Figure 10-20.Examples of Selecting Ports and VLANs as Monitoring Sources**

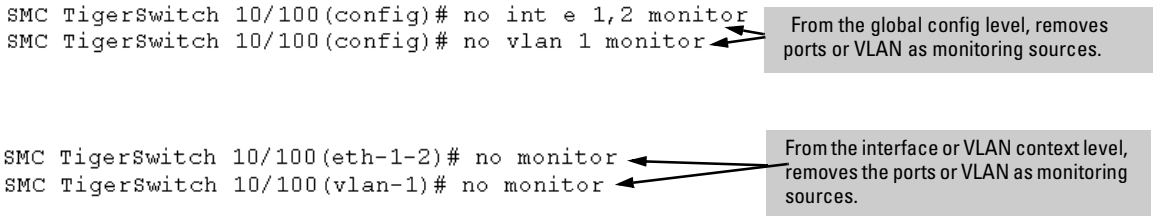



**Figure 10-21.Examples of Removing Ports and VLANs as Monitoring Sources**

## Web: Configuring Port Monitoring

To enable port monitoring:

1. Click on the **Configuration** tab.
2. Click on [Monitor Port].
3. Do either of the following:
   - To monitor a VLAN:
     i. Click on the radio button for **Monitor 1 VLAN**.
     ii. Select the VLAN to monitor.
   - To monitor one or more ports.
     i. Click on the radio button for **Monitor Selected Ports**.
     ii. Select the port(s) to monitor.
4. Click on [Apply Changes].

To remove port monitoring:

1. Click on the Monitoring Off radio button.
2. Click on [Apply Changes].

# 11

# Troubleshooting

This chapter addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the installation guide you received with the switch.)

This chapter includes:


- Troubleshooting Approaches (page 11-2)
- Browser or Console Interface Problems (page 11-3)
- Unusual Network Activity (page 11-5)
  - General Problems (page 11-5)
  - IGMP-Related Problems (page 11-6)
  - Spanning Tree Protocol (STP) Related Problems (page 11-7)
  - VLAN-Related Problems (page 11-8)
- Using the Event Log To Identify Problem Sources (page 11-10)
- Diagnostics and management tools (page 11-13), including:
  - Link test (page 11-13)
  - Ping test (page 11-14)
  - Browse configuration (page 11-17)
  - Command prompt (page 11-12)
  - Restoring the factory default configuration (page 11-19)

# Troubleshooting Approaches

Use these approaches to diagnose switch problems:

- Check the switch LEDs for indications of proper switch operation:
  - Each switch port has a Link LED that should light whenever an active network device is connected to the port.
  - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs.

    See the *Installation Guide* shipped with the switch for a description of the LED behavior and information on using the LEDs for troubleshooting.
- Check the network topology/installation. See the *Installation Guide* shipped with the switch for topology information.
- Check cables for damage, correct type, and proper connections. See the *Installation Guide* shipped with the switch for correct cable types and connector pin-outs.
- Use EliteView (if installed on your network) to help isolate problems and recommend solutions.
- Use the Port Utilization Graph and Alert Log in the web browser interface included in the switch to help isolate problems. See chapter 3, "Using the Web Browser Interface" for operating information. These tools are available through the web browser interface:
  - Port Utilization Graph
  - Alert Log
  - Port Status and Port Counters screens
  - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or Telnet to the switch console. See chapter 4, "Using the Switch Console Interface" for operating information. These tools are available through the switch console
  - Status and Counters screens
  - Event Log
  - Diagnostics tools (Link test, Ping test, configuration file browser, and advanced user commands)

# Browser or Console Access Problems

**Cannot access the web browser interface:**

- Access may be disabled by the **Web Agent Enabled** parameter in the switch console. Check the setting on this parameter by selecting:

  **2. Switch Configuration . . .**

  **1. System Information**

- The switch may not have the correct IP address, subnet mask or gateway. Verify by connecting a console to the switch's Console port and selecting:

  **2. Switch Configuration . . .**

  **1. IP Configuration**

  **Note:** If DHCP/Bootp is used to configure the switch, the IP addressing can be verified by selecting:

  **1. Status and Counters . . .**

  **2. Switch Management Address Information**

  also check the DHCP/Bootp server configuration to verify correct IP addressing.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows web browser access only to a device having an authorized IP address. For more information on IP Authorized managers, see "Using IP Authorized Managers" on page 7-28.
- Java™ applets may not be running on the web browser. They are required for the switch web browser interface to operate correctly. See the online Help on your web browser for how to run the Java applets.

**Cannot Telnet into the switch console from a station on the network:**

- Telnet access may be disabled by the **Inbound Telnet Enabled** parameter in the System Information screen of the menu interface:

  **2. Switch Configuration**

  **1. System Information**

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

  **2. Switch Configuration**

  **5. IP Configuration**

  **Note:** If DHCP/Bootp is used to configure the switch, see the **Note**, above.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see "Enhancing Security By Configuring Authorized IP Managers" on page "Using IP Authorized Managers" on page 7-28.

# Unusual Network Activity

Network activity that exceeds accepted norms may indicate a hardware problem with one or more of the network components, possibly including the switch. Unusual network activity is usually indicated by the LEDs on the front of the switch or measured with the switch console interface or with a network management tool such as EliteView. Refer to the *Installation Guide* you received with the switch for information on using LEDs to identify unusual network activity.

A topology loop can also cause excessive network activity. The event log "FFI" messages can be indicative of this type of problem.

## General Problems

**The network runs slow; processes fail; users cannot access servers or other devices.** Broadcast storms may be occurring in the network. These may be due to redundant links between nodes.

- If you are configuring a port trunk, finish configuring the ports in the trunk before connecting the related cables. Otherwise you may inadvertently create a number of redundant links (i.e. topology loops) that will cause broadcast storms.
- Turn on Spanning Tree Protocol to block redundant links (i.e. topology loops)
- Check for FFI messages in the Event Log.

**Duplicate IP Addresses.** This is indicated by this Event Log message:

> **ip: Invalid ARP source:** *IP address* **on** *IP address*
>
> *where:* both instances of *IP address* are the same address, indicating the switch's IP address has been duplicated somewhere on the network.

**Duplicate IP Addresses in a DHCP Network.** If you use a DHCP server to assign IP addresses in your network and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server "leases" the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, then is subsequently configured to issue

IP addresses that will expire after a limited duration. One solution is to configure "reservations" in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, refer to the documentation for the DHCP server.

One indication of a duplicate IP address in a DHCP network is this Event Log message:

> **ip: Invalid ARP source:** *IP address* **on** *IP address*
>
> *where:* both instances of *IP address* are the same address, indicating the IP address that has been duplicated somewhere on the network.

**The Switch Has Been Configured for DHCP/Bootp Operation, But Has Not Received a DHCP or Bootp Reply.** When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.



## IGMP-Related Problems

**IP Multicast (IGMP) Traffic That Is Directed By IGMP Does Not Reach IGMP Hosts or a Multicast Router Connected to a Port.** IGMP must be enabled on the switch and the affected port must be configured for "Auto" or "Forward" operation.

**IP Multicast Traffic Floods Out All Ports; IGMP Does Not Appear To Filter Traffic.** The IGMP feature does not operate if the switch or VLAN does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch or VLAN, do either of the following:

- **Try Using the Web Browser Interface:** If you can access the web browser interface, then an IP address is configured.
- **Try To Telnet to the Switch Console:** If you can Telnet to the switch, then an IP address is configured.
- **Using the Switch Console Interface:** From the Main Menu, check the Management Address Information screen by clicking on

  **1. Status and Counters**

  **2. Switch Management Address Information**

## Problems Related to Spanning-Tree Protocol (STP)

**Caution**

If you enable STP, it is recommended that you leave the remainder of the STP parameter settings at their default values until you have had an opportunity to evaluate STP performance in your network. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. To learn the details of STP operation, refer to the IEEE 802.1d standard.

**Broadcast Storms Appearing in the Network.** This can occur when there are physical loops (redundant links) in the topology.Where this exists, you should enable STP on all bridging devices in the topology in order for the loop to be detected.

**STP Blocks a Link in a VLAN Even Though There Are No Redundant Links in that VLAN.** In 802.1Q-compliant switches such as the SMC6624M, STP blocks redundant physical links even if they are in separate VLANs. A solution is to use only one, multiple-VLAN (tagged) link between the devices. Also, if ports are available, you can improve the bandwidth in this situation by using a port trunk. See "STP Operation with 802.1Q VLANs" on page 9-107.

## Stacking-Related Problems

**The Stack Commander Cannot Locate any Candidates.** Stacking operates on the primary VLAN, which in the default configuration is the DEFAULT_VLAN. However, if another VLAN has been configured as the primary VLAN, and the Commander is not on the primary VLAN, then the Commander will not detect Candidates on the primary VLAN.

## Timep or Gateway Problems

**The Switch Cannot Find the Timep Server or the Configured Gateway .** Timep and Gateway access are through the primary VLAN, which in the default configuration is the DEFAULT_VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

## VLAN-Related Problems

**Monitor Port.** When using the monitor port in a multiple VLAN environment, it can be useful to know how broadcast, multicast, and unicast traffic is tagged. The following table describes the tagging to expect.

| | Within Same Tagged VLAN as Monitor Port | Within Same Untagged VLAN as Monitor Port | Outside of Tagged Monitor Port VLAN | Outside of Untagged Monitor Port VLAN |
|---|---|---|---|---|
| Broadcast | Tagged | Untagged | Untagged | Untagged |
| Multicast | Tagged | Untagged | Untagged | Untagged |
| Unicast Flood | Tagged | Untagged | Untagged | Untagged |
| Unicast Not to Monitor Port | Untagged | Untagged | Untagged | Untagged |
| Unicast to Monitor Port | Tagged | Untagged | N/A—Dropped | N/A—Dropped |

**None of the devices assigned to one or more VLANs on an 802.1Q-compliant switch are being recognized.** If multiple VLANs are being used on ports connecting 802.1Q-compliant devices, inconsistent VLAN IDs may have been assigned to one or more VLANs. For a given VLAN, the same VLAN ID must be used on all connected 802.1Q-compliant devices.

**Link Configured for Multiple VLANs Does Not Support Traffic for One or More VLANs.** One or more VLANs may not be properly configured as "Tagged" or "Untagged". A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured the same on both ports. For example, VLAN_1 and VLAN_2 use the same link between switch "X" and switch "Y".

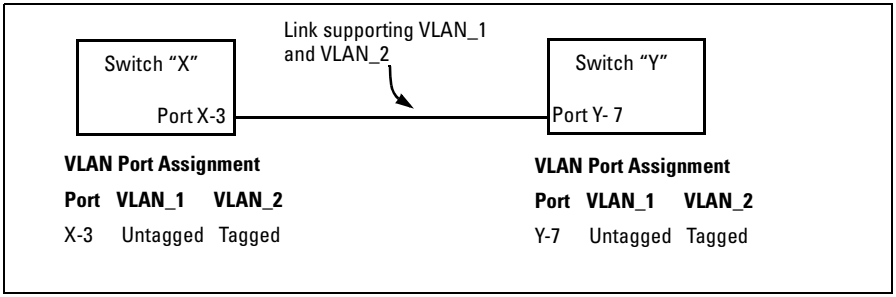


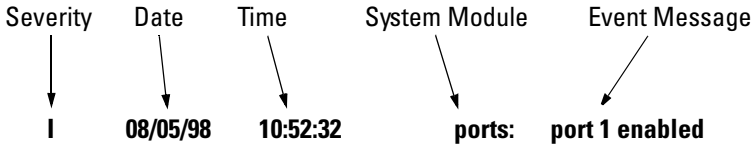

**Figure 11-1. Example of Correct VLAN Port Assignments on a Link**

1. If VLAN_1 (VID=1) is configured as “Untagged” on port 3 on switch “X”, then it must also be configured as “Untagged” on port 7 on switch “Y”. Make sure that the VLAN ID (VID) is the same on both switches.
2. Similarly, if VLAN_2 (VID=2) is configured as “Tagged on the link port on switch “A”, then it must also be configured as “Tagged” on the link port on switch “B”. Make sure that the VLAN ID (VID) is the same on both switches.

**Duplicate MAC Addresses Across VLANs.** Duplicate MAC addresses on different VLANs are not supported and can cause VLAN operating problems. There are no explicit events or statistics to indicate the presence of duplicate MAC addresses in a VLAN environment. However, one symptom that may occur is that a duplicate MAC address can appear in the Port Address Table of one port, and then later appear on another port. (This can also occur in a LAN where there are redundant paths between nodes and Spanning Tree is turned off.) For more information, refer to “VLAN Restrictions” on page 9-73.

# Using the Event Log To Identify Problem Sources

The Event Log records operating events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each Event Log entry is composed of five fields:




***Severity*** is one of the following codes:

- **I** (information) indicates routine events.
- **W** (warning) indicates that a service has behaved unexpectedly.
- **C** (critical) indicates that a severe switch error has occurred.
- **D** (debug) reserved for SMC internal diagnostic information.

***Date*** is the date in *mm/dd/yy* format that the entry was placed in the log.

***Time*** is the time in *hh:mm:ss* format that the entry was placed in the log.

***System Module*** is the internal module (such as "ports" for port manager) that generated the log entry. If VLANs are configured, then a VLAN name also appears for an event that is specific to an individual VLAN. Table 11-1 on page 11-11 lists the individual modules.

***Event Message*** is a brief description of the operating event.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line each time a new line is received. The event log window contains 14 log entry lines and can be positioned to any location in the log.

The event log will be *erased* if power to the switch is interrupted.

(The event log is *not* erased by using the **Reboot Switch** command in the Main Menu.)

**Table 11-1. Event Log System Modules**

| Module | Event Description | Module | Event Description |
|---|---|---|---|
| addrMgr | Address table | mgr | Console management |
| chassis | switch hardware | ports | Change in port status; static trunks |
| bootp | bootp addressing | snmp | SNMP communications |
| console | Console interface | stack | Stacking |
| dhcp | DHCP addressing | stp | Spanning Tree |
| download | file transfer | sys, system | Switch management |
| FFI | Find, Fix, and Inform) -- available in the console event log and web browser interface alert log | telnet | Telnet activity |
| garp | GARP/GVRP | tcp | Transmission control |
| igmp | IP Multicast | tftp | File transfer for new OS or config. |
| ip | IP-related | timep | Time protocol |
| ipx | Novell Netware | vlan | VLAN operations |
| lacp | Dynamic LACP trunks | Xmodem | Xmodem file transfer |



## Menu: Entering and Navigating in the Event Log

From the Main Menu, select **Event Log**.

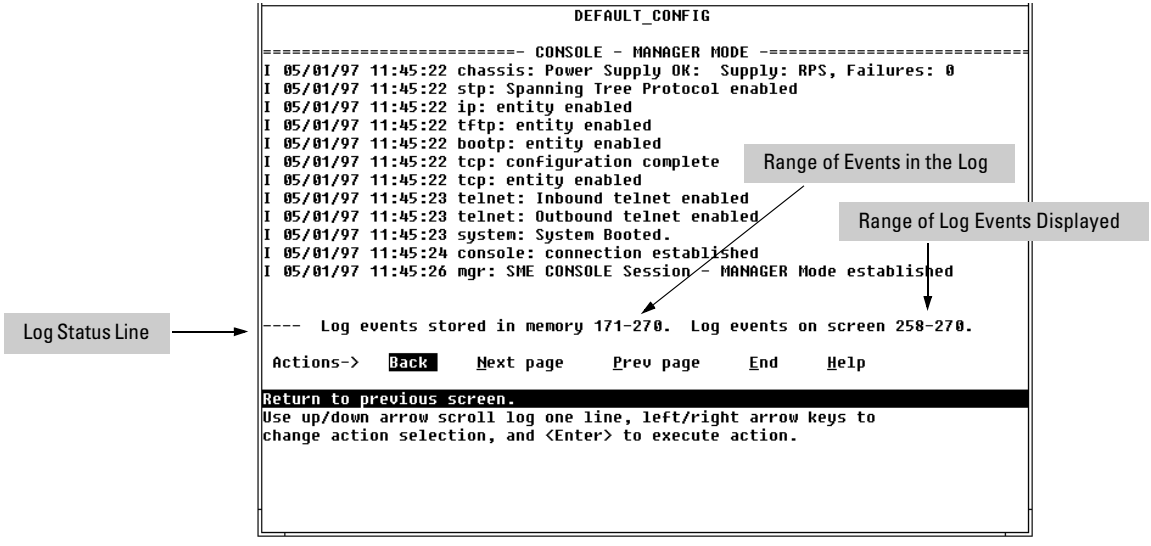



**Figure 11-2. Example of an Event Log Display**

The *log status line* at the bottom of the display identifies where in the sequence of event messages the display is currently positioned.

To display various portions of the Event Log, either preceding or following the currently visible portion, use either the actions listed at the bottom of the display (**Next page**, **Prev page**, or **End**), or the keys described in the following table:

**Table 11-2. Event Log Control Keys**

| Key | Action |
|---|---|
| [N] | Advance the display by one page (next page). |
| [P] | Roll back the display by one page (previous page). |
| ↓ | Advance display by one event (down one line). |
| ↑ | Roll back display by one event (up one line). |
| [E] | Advance to the end of the log. |
| [H] | Display Help for the event log. |



## CLI:

Using the CLI, you can list

- Events recorded since the last boot of the switch
- All events recorded
- Event entries containing a specific keyword, either since the last boot or all events recorded

***Syntax:*** show logging [-a] [<search-text>]

| | |
|---|---|
| SMC TigerSwitch 10/100> show logging | Lists recorded log messages since last reboot. |
| SMC TigerSwitch 10/100> show logging -a | Lists all recorded log messages. |
| SMC TigerSwitch 10/100> show logging -a system | Lists all log messages having "system" in the text or module name. |
| SMC TigerSwitch 10/100> show logging system | Lists all log messages since the last reboot that have "system" in the text or module name. |

# Diagnostic Tools

**Diagnostic Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| PingTest | n/a | — | page 11-15 | page 11-14 |
| Link Test | n/a | — | page 11-15 | page 11-14 |
| Display Config File | n/a | — | page 11-17 | page 11-17 |
| Admin. and Troubleshooting Commands | n/a | — | page 11-18 | — |
| Factory-Default Config | page 11-19 (Buttons) | — | page 11-19 | — |

## Ping and Link Tests

The Ping test and the Link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

**Note**

To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

**Ping Test.** This is a test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests).

**Link Test.** This is a test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured). During the link test, IEEE 802.2 test packets are sent to the designated network device in the same VLAN or broadcast domain. The remote device must be able to respond with an 802.2 Test Response Packet.

## Web: Executing Ping or Link Tests

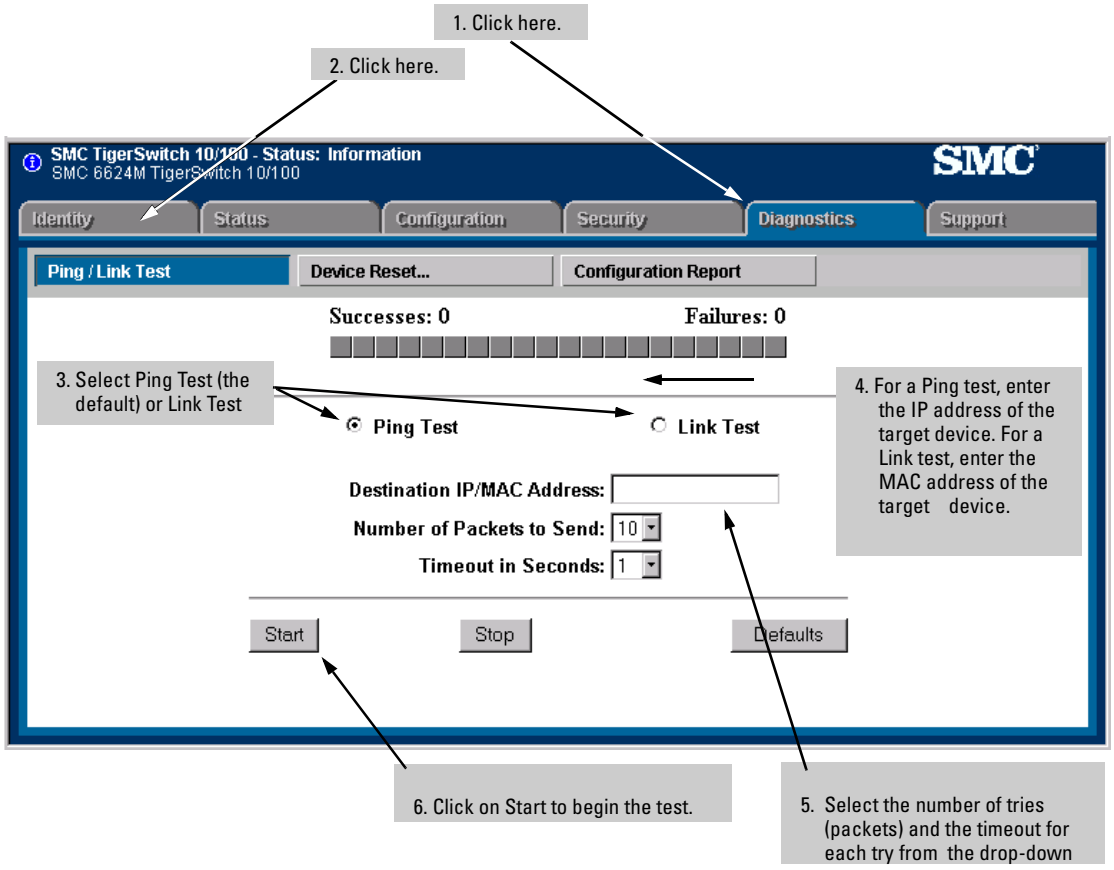



**Figure 11-12.Link and Ping Test Screen on the Web Browser Interface**

**Successes** indicates the number of Ping or Link packets that successfully completed the most recent test.

**Failures** indicates the number of Ping or Link packets that were unsuccessful in the last test. Failures indicate connectivity or network performance problems (such as overloaded links or devices).

**Destination IP/MAC Address** is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the X.X.X.X format where X is a decimal number between 0 and 255. A MAC address is made up of 12 hexadecimal digits, for example, 0060b0-080400.

**Number of Packets to Send** is the number of times you want the switch to attempt to test a connection.

**Timeout in Seconds** is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

**To halt a Link or Ping test** before it concludes, click on the Stop button. **To reset the screen** to its default settings, click on the Defaults button.

## CLI: Ping or Link Tests

**Ping Tests.** You can issue single or multiple ping tests with varying repititions and timeout periods. The defaults and ranges are:

- Repetitions: 1 (1 - 999)
- Timeout: 5 seconds (1 - 256 seconds)

***Syntax:*** ping <*ip-address*> [repetitions <1 - 999>] [timeout <1 - 256>]

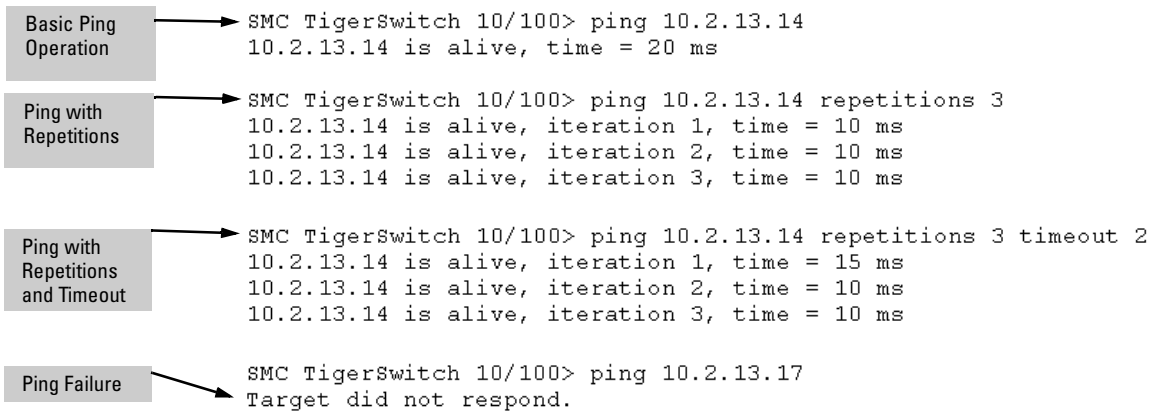



**Figure 11-13.Examples of Ping Tests**

To halt a ping test before it concludes, press [Ctrl] [C].

**Link Tests.** You can issue single or multiple link tests with varying repititions and timeout periods. The defaults are:

- Repetitions: 1 (1 - 9999)
- Timeout: 5 seconds (1 - 256 seconds)

***Syntax:*** link <*mac-address*> [repetitions <1 - 999>] [timeout <1 - 256>]

Basic Link Test

```
SMC TigerSwitch 10/100# link 0030c1-7fcc40
Link-test passed.
```

Link Test with Repetitions

```
SMC TigerSwitch 10/100# link 0030c1-7fcc40 repetitions 3
802.2 TEST packets sent: 3, responses received: 3
```

Link Test with Repetitions and Timeout

```
SMC TigerSwitch 10/100# link 0030c1-7fcc40 repetitions 3 timeout 1
802.2 TEST packets sent: 3, responses received: 3
```

Link Test Over a Specific VLAN

```
SMC TigerSwitch 10/100# link 0030c1-7fcc40 repetitions 3 timeout 1
        vlan 1
302.2 TEST packets sent: 3, responses received: 3
```

Link Test Over a Specific VLAN; Test Fail

```
SMC TigerSwitch 10/100# link 0030c1-7fcc40 repetitions 3 timeout 1
      vlan 222
802.2 TEST packets sent: 3, responses received: 0
```

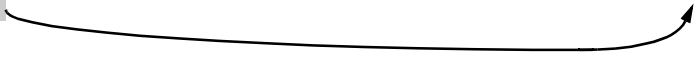


**Figure 11-14.Example of Link Tests**

# Displaying the Configuration File

The complete switch configuration is contained in a file that you can browse from either the web browser interface or the CLI. It may be useful in some troubleshooting scenarios to view the switch configuration.

## CLI: Viewing the Configuration File

Using the CLI, you can display either the running configuration or the startup configuration. (For more on these topics, see appendix C, "Switch Memory and Configuration".)

| | | |
|---|---|---|
| ***Syntax:*** | write terminal | Displays the running configuration. |
| | show config | Displays the startup configuration. |

## Web: Viewing the Configuration File

To display the running configuration,  through the web browser interface:

1. Click on the **Diagnostics** tab.
2. Click on [Configuration Report]
3. Use the right-side scroll bar to scroll through the configuration listing.

## CLI Administrative and Troubleshooting Commands

These commands provide information or perform actions that you may find helpful in troubleshooting operating problems with the switch.

**Note**

For more on the CLI, refer to chapter 3, "Using the Command Line Reference (CLI)."

| | | |
|---|---|---|
| ***Syntax:*** | show version | Shows the software version currently running on the switch. |
| | show boot-history | Displays the switch shutdown history. |
| | show history | Displays the current command history. |
| | [no] page | Toggles the paging mode for display commands between continuous listing and per-page listing. |
| | Setup | Displays the Switch Setup screen from the menu interface |
| | Repeat | Repeatedly executes the previous command until a key is pressed. |
| | kill | Terminates all other active sessions. |

# Restoring the Factory-Default Configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process momentarily interrupts the switch operation, clears any passwords, clears the console event log, resets the network counters to zero, performs a complete self test, and reboots the switch into its factory default configuration including deleting an IP address. There are two methods for restting to the factory-default configuration:

- CLI
- Clear/Reset button combination

**Note**

SMC recommends that you save your configuration to a TFTP server before resetting the switch to its factory-default configuration. You can also save your configuration via Xmodem, to a directly connected PC.



## CLI: Resetting to the Factory-Default Configuration

This command operates at any level *except* the Operator level.

***Syntax:*** erase startup-configuration — Deletes the startup-config file in flash so that the switch will reboot with its factory-default configuration.

## Clear/Reset: Resetting to the Factory-Default Configuration

To execute the factory default reset, perform these steps:

1. Using pointed objects, simultaneously press both the Reset and Clear buttons on the front of the switch.
2. Continue to press the Clear button while releasing the Reset button.
3. When the Self Test LED begins to flash, release the Clear button.

   The switch will then complete its self test and begin operating with the configuration restored to the factory default settings.

# Transferring an Operating System or Startup Configuration File

You can download new switch software (operating system—OS) and upload or download switch configuration files. These features are useful for acquiring periodic switch software upgrades and for storing or retrieving a switch configuration.

This appendix includes the following information:

- downloading an operating system (this page)
- transferring switch configurations (page A-9)

## Downloading an Operating System (OS)

SMC periodically provides switch operating system (OS) updates through the SMC website (http://www.smc.com). After you acquire the new OS file, you can use one of the following methods for downloading the operating system (OS) code to the switch:

- The TFTP feature (**Download OS**) command in the Main Menu of the switch console interface (page A-2)
- A switch-to-switch file transfer
- Xmodem transfer method

**Note**

Downloading a new OS does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model. See “Transferring Switch Configurations” on page A-9.

## Using TFTP To Download the OS File from a Server

This procedure assumes that:

- An OS file for the switch has been stored on a TFTP server accessible to the switch. (The OS file is typically available from SMC's web site—http://www.smc.com.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the OS file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the OS file stored in the TFTP server for the switch (for example, A_01_01.swi).

**Note**

*If your TFTP server is a Unix workstation, ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the OS filenames on the server.*

## Menu: TFTP Download from a Server

1. In the console Main Menu, select **Download OS** to display this screen:

```
========================== CONSOLE - MANAGER MODE ============================
                                Download OS

  Current Firmware revision : F.01.XX

  Method [TFTP] : TFTP
  TFTP Server :

  Remote File Name :



 Actions->   Cancel     Edit     eXecute     Help

Select the file transfer method (TFTP and XMODEM are currently supported).
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure A-1. Example of the Download OS Screen (Default Values)**

2. Press [E] (for **Edit**).
3. Ensure that the **Method** field is set to **TFTP** (the default).
4. In the **TFTP Server** field, type in the IP address of the TFTP server in which the OS file has been stored.
5. In the **Remote File Name** field, type the name of the OS file. If you are using a UNIX system, remember that the filename is case-sensitive.
6. Press [Enter], then [X] (for **eXecute**) to begin the OS download. The following screen then appears:

```
========================== CONSOLE - MANAGER MODE ============================
                                Download OS
  Current Firmware revision : F.01.02
  Method [TFTP] : TFTP
  TFTP Server : 13.28.227.105

  Remote File Name : F_01_03.swi


              Received 370,000 bytes of OS download.
  +-------------------------------------------------------------------+
  |*******************                                                |
  +-------------------------------------------------------------------+
```

**Figure A-2. Example of the Download OS Screen During a Download**

A "progress" bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and you will see **Validating and writing system software to FLASH...** followed by **Transfer completed**.

After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.

7. To confirm that the operating system downloaded correctly:
   a. From the Main Menu, select **1. Status and Counters**, and from the Status and Counters menu, select **1. General System Information**
   b. Check the **Firmware revision** line.

### CLI: TFTP Download from a Server

***Syntax:*** copy tftp flash <*ip-address*> <*remote-os-file*>

For example, to download an OS file named F_2_02.swi from a TFTP server with the IP address of 10.2.3.9:

1. Execute the copy command as shown below:

```
SMC TigerSwitch 10/100# copy tftp flash 10.2.3.9 F_2_02.swi
Device will be rebooted, do you want to continue [y/n]?  y
00224K _
```

2. When the switch finishes downloading the OS file from the server, it displays this progress message:

   **Validating and Writing System Software to FLASH . . .**

3. After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

## Switch-to-Switch Download

If you have two or more SMC6624M switches networked together, you can download the OS software from one switch to another by using the Download OS feature in the switch console interface.

### Menu: Switch-to-Switch Download

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS** screen.

2. Ensure that the **Method** parameter is set to **TFTP** (the default).
3. In the **TFTP Server** field, enter the IP address of the remote SMC6624M switch containing the OS you want to download.
4. Enter "**flash**" for the **Remote File Name**. (Type "**flash**" in lowercase characters.)
5. Press [Enter], then [X] (for **eXecute**) to begin the OS download.
6. A "progress" bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and the following messages appear:

   **Validating and writing system software to FLASH...**

   **Transfer completed**

   After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.
7. To confirm that the operating system downloaded correctly:
   a. From the Main Menu, select

      **Status and Counters**

         **General System Information**

   b. Check the **Firmware revision** line.

## CLI: Switch-To-Switch Download

Syntax: copy tftp flash <ip-addr> flash

For example, to download an OS file from an SMC6624M with an IP address of 10.28.227.103:

```
SMC TigerSwitch 10/100# copy tftp flash 13.29.227.103 flash
Device will be rebooted, do you want to continue [y/n]?  y
00117K _
```

Running Total of Bytes Downloaded

**Figure 8-3. Switch-To-Switch OS Download Using the CLI**

## Using Xmodem to Download the OS File From a PC

This procedure assumes that:

- The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch operating system (OS) is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the Windows NT terminal emulator, you would use the **Send File** option in the **Transfer** dropdown menu.)

### Menu: Xmodem Download

1. From the console Main Menu, select

   **7. Download OS**

2. Press [E] (for **Edit**).
3. Use the Space bar to select **XMODEM** in the **Method** field.
4. Press [Enter], then [X] (for **eXecute**) to begin the OS download. The following message then appears:

   **Press enter and then initiate Xmodem transfer**
   **from the attached computer.....**

5. Execute the terminal emulator command(s) to begin Xmodem binary transfer.

   The download can take several minutes, depending on the baud rate used for the transfer.

6. When the download finishes, the switch automatically reboots itself and begins running the new OS version.
7. To confirm that the operating system downloaded correctly:
   a. From the Main Menu, select

      **1. Status and Counters**
         **1. General System Information**

   b. Check the **Firmware revision** line.

### CLI: Xmodem Download from a PC or Unix Workstation

***Syntax:*** copy xmodem flash <unix | pc>

For example, to download an OS file named F_01_03.swi from a PC:

1. Execute the following command in the CLI:

```
SMC TigerSwitch 10/100# copy xmodem flash pc
Device will be rebooted, do you want to continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...
```

2. Execute the terminal emulator commands to begin the Xmodem transfer.

   The download can take several minutes, depending on the baud rate used in the transfer.

   When the download finishes, the switch automatically reboots itself and begins running the new OS version.

3. To confirm that the operating system downloaded correctly:

   ```
   SMC TigerSwitch 10/100> show system
   ```

   Check the **Firmware revision** line.

# Troubleshooting TFTP Downloads

If a TFTP download fails, the Download OS screen indicates the failure.

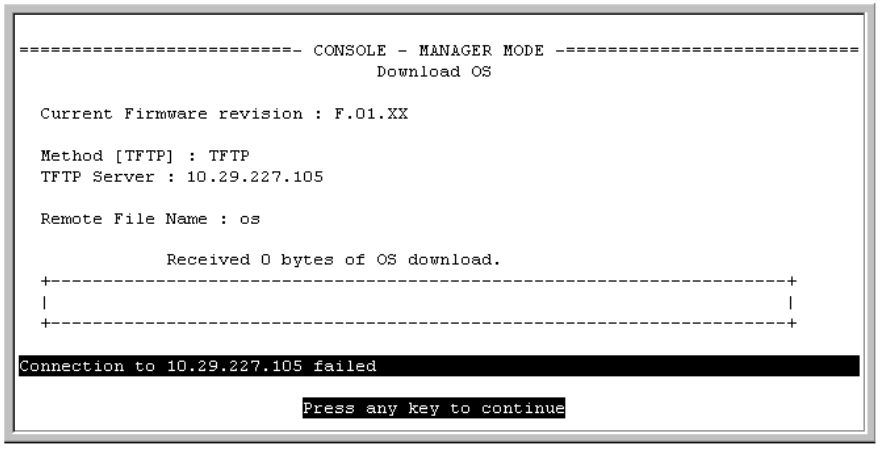



**Figure A-4. Example of Message for Download Failure**

To find more information on the cause of a download failure, examine the messages in the switch's Event Log by executing this CLI command:

```
SMC TigerSwitch 10/100# show log tftp
```

(For more on the Event Log, see "Using the Event Log To Identify Problem Sources" on page 11-10.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a Unix machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the Download OS screen.
- One or more of the switch's IP configuration parameters are incorrect.
- For a Unix TFTP server, the file permissions for the OS file do not allow the file to be copied.

- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

**Note**

If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself. In this case, an appropriate message is displayed in the copyright screen that appears after the switch reboots.

# Transferring Switch Configurations

**Transfer Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| use TFTP to copy a configuration from a remote host to the startup-config file | n/a | — | below | |
| use TFTP to copy the startup-config file to a remote host | n/a | — | page A-10 | |
| use Xmodem to copy a configuration from a serially connected host to the startup-config file | n/a | — | page A-10 | |
| Use Xmodem to copy the startup-config file to a serially connected host | n/a | — | page A-11 | |

Using the CLI commands described in this section, you can copy switch configurations to and from a switch.

### TFTP: Retrieving a Configuration from a Remote Host.

***Syntax:*** copy tftp startup-config <*ip-address*> <*remote-file*>

This command copies a configuration from a remote host to the startup-config file in the switch. (See appendix C, "Switch Memory and Configuration" for information on the startup-config file.)

For example, to download a configuration file named **sw2512** in the **configs** directory on drive "**d**" in a remote host having an IP address of 13.28.227.105:

```
SMC TigerSwitch 10/100# copy tftp startup-config
13.28.227.105 d:\configs\sw2512
```

**TFTP: Copying a Configuration to a Remote Host.**

***Syntax:*** copy startup-config tftp <*ip-addr*> <*remote-file*>

This command copies the switch's startup configuration (startup-config file) to a remote TFTP host.

For example, to upload the current startup configuration to a file named **sw2512** in the configs directory on drive "**d**" in a remote host having an IP address of 13.28.227.105:

```
SMC TigerSwitch 10/100# copy startup-config tftp
13.28.227.105 d:\configs\sw2512
```

**Xmodem: Copying a Configuration from the Switch to a Serially Connected PC or Unix Workstation.** To use this method, the switch must be connected via the serial port to a PC or Unix workstation to which you want to copy the configuration file. You will need to select a filename, and to know the drive and directory location where you want to store the configuration file.

***Syntax:*** copy startup-config xmodem <pc | unix>

For example, to copy a configuration file to a PC serially connected to the switch:

1. Execute the following command:

```
SMC TigerSwitch 10/100# copy startup-config xmodem pc
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press [Enter].
3. Execute the terminal emulator commands to begin the file transfer.

**Xmodem: Copying a Configuration from a Serially Connected PC or Unix Workstation.** To use this method, the switch must be connected via the serial port to a PC or Unix workstation on which is stored the configuration file you want to copy. To complete the copying, you will need to know the name of the file to copy, and the drive and directory location of the file.

***Syntax:*** copy xmodem startup-config <pc | unix>

For example, to copy a configuration file from a PC serially connected to the switch:

1. Execute the following command:

```
SMC TigerSwitch 10/100# copy xmodem startup-config pc
Device will be rebooted, do you want to continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press [Enter].
3. Execute the terminal emulator commands to begin the file transfer.

When the file transfer finishes, the switch automatically reboots itself with the new configuration.

# MAC Address Management



The switch assigns MAC addresses in these areas:

- For management functions:
  - One Base MAC address assigned to the default VLAN (VID = 1)
  - Additional MAC address(es) corresponding to additional VLANs you configure in the switch
- For internal switch operations: One MAC address per port (See "CLI: Viewing the Port and VLAN MAC Addresses" on page B-3.)

MAC addresses are assigned at the factory. The switch automatically implements these addresses for VLANs and ports as they are added to the switch.

**Note** The switch's base MAC address is also printed on a label affixed to the back of the switch.

## Determining MAC Addresses

**MAC Address Viewing Methods**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view switch's base (default vlan) MAC address and the addressing for any added VLANs | n/a | B-2 | B-3 | — |
| view port MAC addresses (hexadecimal format) | n/a | — | B-3 | — |

**Use the menu interface** to view the switch's base MAC address and the MAC address assigned to any non-default VLAN you have configured on the switch.

**Note** The switch's base MAC address is used for the default VLAN (VID = 1) that is always available on the switch.

**Use the CLI** to view the switch's port MAC addresses in hexadecimal format.

## Menu: Viewing the Switch's MAC Addresses

The Management Address Information screen lists the MAC addresses for:

- Base switch (default VLAN; VID = 1)
- Any additional VLANs configured on the switch.

Also, the Base MAC address appears on a label on the back of the switch.

**Note**

The Base MAC address is used by the first (default) VLAN in the switch. This is usually the VLAN named "DEFAULT_VLAN" unless the name has been changed (by using the VLAN Names screen). On the SMC6624M, the VID (VLAN identification number) for the default VLAN is always "1", *and cannot be changed.*

**To View the MAC Address (and IP Address) assignments for VLANs Configured on the Switch:**

1. From the Main Menu, Select

   **1. Status and Counters**

   **2. Switch Management Address Information**

   If the switch has only the default VLAN, the following screen appears. If the switch has multiple static VLANs, each is listed with its address data.

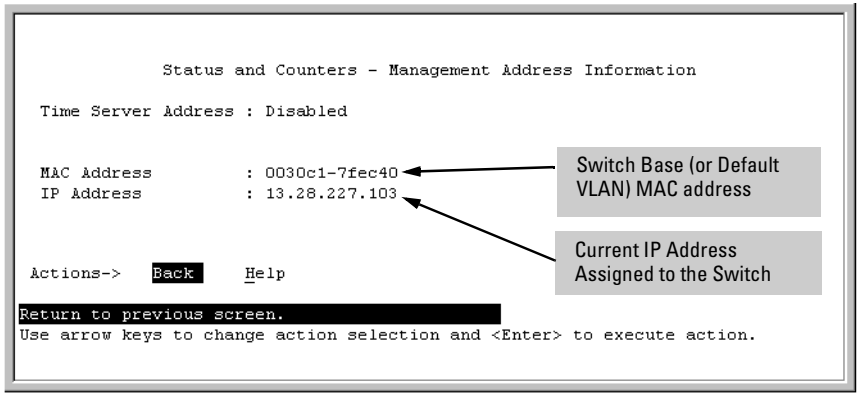



**Figure B-1. Example of the Management Address Information Screen**

## CLI: Viewing the Port and VLAN MAC Addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control and the Spanning Tree Protocol. Determining the MAC address assignments for individual ports can sometimes be useful when diagnosing switch operation. To display these addresses, use the **walkmib** command at the command prompt:

**Note**

This procedure displays the MAC addresses for all ports and existing VLANs in the switch, regardless of which VLAN you select.

1. If the switch is at the CLI Operator level, use the **enable** command to enter the Manager level of the CLI.
2. Type the following command to display the MAC address for each port on the switch:

   ```
   SMC TigerSwitch 10/100# walkmib ifPhysAddress
   ```

   (The above command is not case-sensitive.)

The following figure is an example of the display:

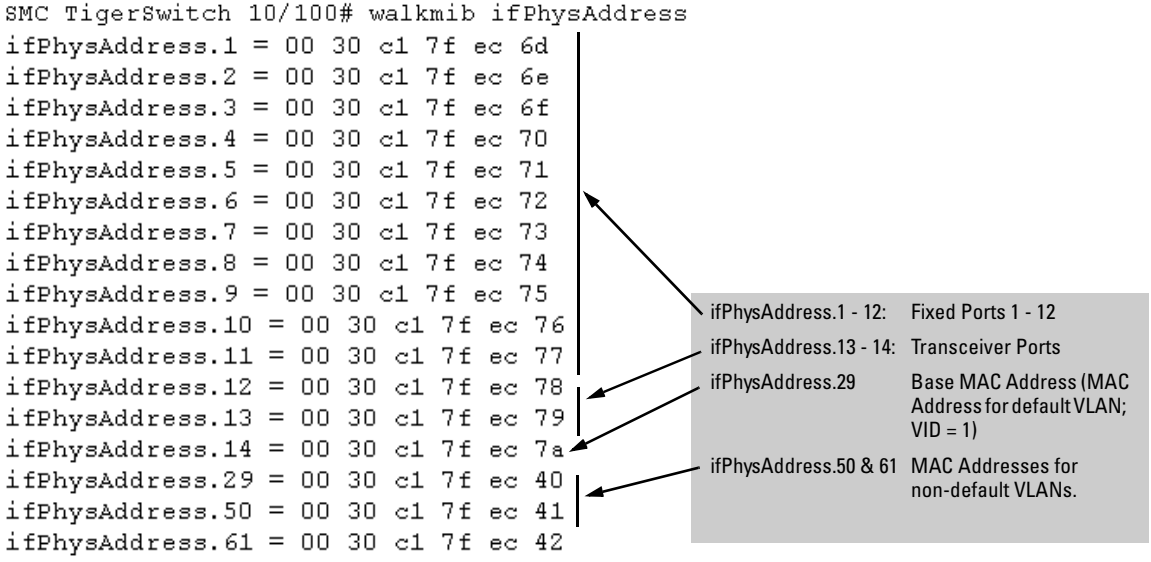



**Figure B-2. Example of Port MAC Address Assignments**

# Switch Memory and Configuration

This appendix describes the following:

- How switch memory manages configuration changes
- How the CLI implements configuration changes
- How the menu interface and web browser interface implement configuration changes



## Overview of Configuration File Management

The switch maintains two configuration files, the *running-config* file and the *startup-config* file.

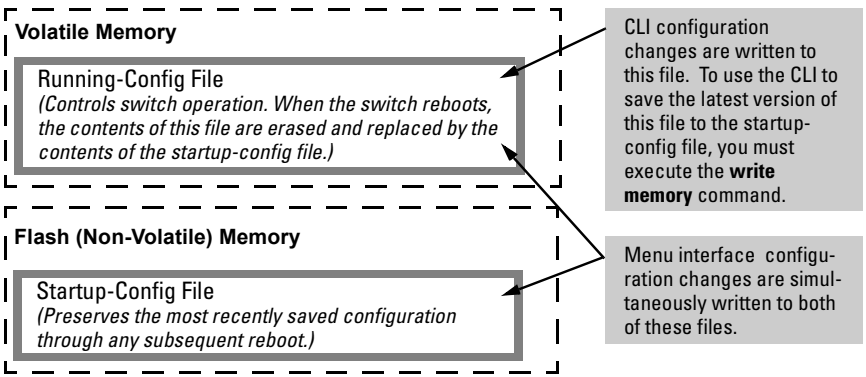



**Figure C-1. Conceptual Illustration of Switch Memory Operation**

- **Running Config File:** Exists in volatile memory and controls switch operation. If no configuration changes have been made in the CLI since the switch was last booted, the running-config file is identical to the startup-config file.

- **Startup-config File:** Exists in flash (non-volatile) memory and is used to preserve the most recently-saved configuration as the "permanent" configuration.

Rebooting the switch replaces the current running-config file with a new running-config file that is an exact copy of the current startup-config file.

**Note**

Any of the following actions reboots the switch:

- Executing the **boot** or the **reload** command in the CLI
- Executing the **Reboot** command in the menu interface
- Pressing the Reset button on the front of the switch
- Removing, then restoring power to the switch



**Options for Saving a New Configuration.** Making one or more changes to the running-config file creates a new operating configuration. *Saving* a new configuration means to overwrite (replace) the current startup-config file with the current running-config file. This means that if the switch subsequently reboots for any reason, it will resume operation using the new configuration instead of the configuration previously defined in the startup-config file. There are three ways to save a new configuration:

- **In the CLI:** Use the **write memory** command. This overwrites the current startup-config file with the contents of the current running-config file.
- **In the menu interface:** Use the **Save** command. This overwrites *both* the running-config file and the startup-config file with the changes you have specified in the menu interface screen.
- **In the web browser interface:** Use the [Apply Changes] button or other appropriate button. This overwrites *both* the running-config file and the startup-config file with the changes you have specified in the web browser interface window.

Note that using the CLI instead of the menu or web browser interface gives you the option of changing the running configuration without affecting the startup configuration. This allows you to test the change without making it "permanent". When you are satisfied that the change is satisfactory, you can make it permanent by executing the **write memory** command. For example, suppose you use the following command to disable port 5:

```
SMC TigerSwitch 10/100(config)# interface ethernet 5
disable
```

The above command disables port 5 in the running-config file, but not in the startup-config file. Port 5 remains disabled only until the switch reboots. If you want port 5 to remain disabled through the next reboot, use **write memory** to save the current running-config file to the startup-config file in flash memory.

```
SMC TigerSwitch 10/100(config)# write memory
```

**Storing and Retrieving Configuration Files.** You can store or retrieve a backup copy of the startup-config file on another device. For more information, see appendix A, "Transferring an Operating System or Startup-Config File."



# Using the CLI To Implement Configuration Changes

The CLI offers these capabilities:

- Access to the full set of switch configuration features
- The option of testing configuration changes before making them permanent

**How To Use the CLI To View the Current Configuration Files.** Use **show** commands to view the configuration for individual features, such as port status or Spanning Tree Protocol. However, to view either the entire startup-config file or the entire running-config file, use the following commands:

- **show startup-config**: Displays the current startup-config file.
- **write terminal**: Displays the current running-config file.

**Note**

The **show startup-config** and **write terminal** commands display the configuration settings that differ from the switch's factory-default configuration.

**How To Use the CLI To Reconfigure Switch Features.** Use this procedure to permanently change the switch configuration (that is, to enter a change in the startup-config file).

1. Use the appropriate CLI commands to reconfigure the desired switch parameters. This updates the selected parameters in the running-config file.

2. Use the appropriate **show** commands to verify that you have correctly made the desired changes.
3. Observe the switch's performance with the new parameter settings to verify the effect of your changes.
4. When you are satisfied that you have the correct parameter settings, use the **write memory** command to copy the changes to the startup-config file.

***Syntax:*** `write memory`

For example, the default port mode setting is **auto**. Suppose that your network uses Cat 3 wiring and you want to connect the switch to another autosensing device capable of 100 Mbps operation. Because 100 Mbps over Cat 3 wiring can introduce transmission problems, the recommended port mode is **auto-10**, which allows the port to negotiate full- or half-duplex, but restricts speed to 10 Mbps. The following command configures port 5 to auto-10 mode in the running-config file, allowing you to observe performance on the link without making the mode change permanent.

```
SMC TigerSwitch 10/100(config)# interface e 5 speed-
duplex auto-10
```

After you are satisfied that the link is operating properly, you can save the change to the switch's permanent configuration (the startup-config file) by executing the following command:

```
SMC TigerSwitch 10/100(config)# write memory
```

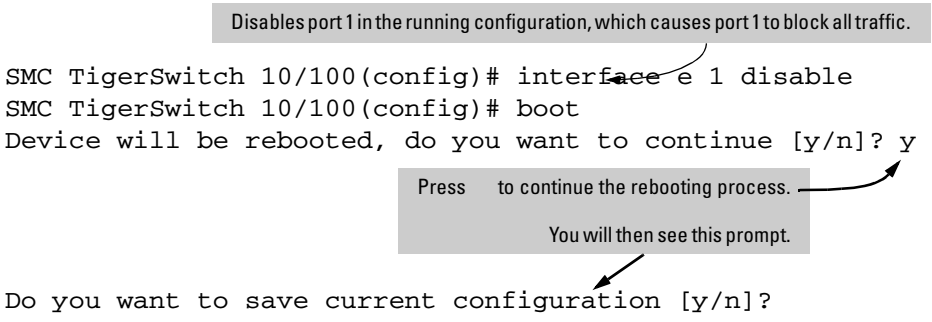
The new mode (**auto-10**) on port 5 is now saved in the startup-config file, and the startup-config and running-config files are identical. If you subsequently reboot the switch, the **auto-10** mode configuration on port 5 will remain because it is included in the startup-config file.

### How To Cancel Changes You Have Made to the Running-Config File.

If you use the CLI to change parameter settings in the running-config file, and then decide that you don't want those changes to remain, you can use either of the following methods to remove them:

- Manually enter the earlier values you had for the changed settings. (This is recommended if you want to restore a small number of parameter settings to their previous boot-up values.)
- Update the running-config file to match the startup-config file by rebooting the switch. (This is recommended if you want to restore a larger number of parameter settings to their previous boot-up values.)

If you use the CLI to change a parameter setting, and then execute the **boot** command without first executing the **write memory** command to save the change, the switch prompts you to specify whether to save the changes in the current running-config file. For example:




The above prompt means that one or more parameter settings in the running-config file differ from their counterparts in the startup-config file and you need to choose which config file to retain and which to discard.

- If you want to update the startup-config file to match the running-config file, press [Y] for "yes". (This means that the changes you entered in the running-config file will be saved in the startup-config file.)
- If you want to discard the changes you made to the running-config file so that it will match the startup-config file, then press [N] for "no". (This means that the switch will discard the changes you entered in the running-config file and will update the running-config file to match the startup-config file.)

**Note**

If you use the CLI to make a change to the running-config file, you must use the **write memory** command to save the change to the startup-config file. That is, if you use the CLI to change a parameter setting, but then reboot the switch from either the CLI or the menu interface without first executing the **write memory** command in the CLI, the current startup-config file will replace the running-config file, and any changes in the running-config file will be lost.

Also, where a parameter setting is accessable from both the CLI and the menu interface, if you change the setting in the CLI, the new value will appear in the menu interface display for that parameter. *However, only the* **write memory** *command in the CLI will actually save the change to the startup-config file. Using the* **Save** *command in the menu interface will not save a change made to the running config by the CLI.*

**How To Reset the startup-config and running-config Files to the Factory Default Configuration.** This command reboots the switch, replacing the contents of the current startup-config and running-config files with the factory-default startup configuration.

***Syntax:*** `erase startup-config`

For example:

```
SMC TigerSwitch 10/100(config)# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?
```

Press [Y] to replace the current configuration with the factory default configuration and reboot the switch. Press [N] to retain the current configuration and prevent a reboot.



# Using the Menu and Web Browser Interfaces To Implement Configuration Changes

The menu and web browser interfaces offer these advantages:

- Quick, easy menu or window access to a subset of switch configuration features (See the "Menu Features List" on page 2-13 and the web browser "General Features" list on page .)
- Viewing several related configuration parameters in the same screen, with their default and current settings
- Immediately changing both the running-config file and the startup-config file with a single command

## Using the Menu Interface To Implement Configuration Changes

You can use the menu interface to simultaneously save and implement a subset of switch configuration changes without having to reboot the switch. That is, when you save a configuration change in the menu interface, you simultaneously change both the running-config file and the startup-config file.

**Note**

The only exception to this operation are two VLAN-related parameter changes that require a reboot—described under "Rebooting To Activate Configuration Changes" on page C-8.

## Using **Save** and **Cancel** in the Menu Interface

For any configuration screen in the menu interface, the Save command:

1. Implements the changes in the running-config file
2. Saves your changes to the startup-config file

If you decide not to save and implement the changes in the screen, select **Cancel** to discard them and continue switch operation with the curent operation. For example, suppose you have made the changes shown below in the System Information screen:

To save and implement the changes for all parameters in this screen, press the key, then press (for **Save**). To cancel all changes, press the key, then press (for **Cancel**)

```
SMC6624M                                                    1-Jan-1990   1:24:00
==========================- CONSOLE - MANAGER MODE -============================
                    Switch Configuration - System Information

  System Name : SMC6624M
  System Contact : Extension 5440
  System Location : System Support Office, Rm 231

  Inactivity Timeout (min) [0] : 0      MAC Age Interval (sec) [300] : 300
  Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes

  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled

  Time Zone [0] : 8
  Daylight Time Rule [None] : Continental-US-and-Canada


 Actions->   Cancel     Edit     Save     Help

Select Daylight Time Rule for your location.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure 2-2. Example of Pending Configuration Changes that Can Be Saved or Cancelled**

**Note**

If you reconfigure a parameter in the CLI and then go to the menu interface without executing a **write memory** command, those changes are stored only in the running configuration (even if you execute a Save operation in the menu interface). If you then execute a switch reboot command in the menu inter-

face, the switch discards the configuration changes made while using the CLI. To ensure that changes made while using the CLI are saved, execute **write memory** in the CLI before rebooting the switch.

## Rebooting from the Menu Interface

- Terminates the current session and performs a reset of the operating system
- Activates any configuration changes that require a reboot
- Resets statistical counters to zero

(Note that statistical counters can be reset to zero without rebooting the switch. See "Displaying Port Counters" on page 10-8.)

To Reboot the switch, use the **Reboot Switch** option in the Main Menu. (Note that the Reboot Switch option is not available if you log on in Operator mode; that is, if you enter an Operator password instead of a manager password at the password prompt.)



Reboot Switch option

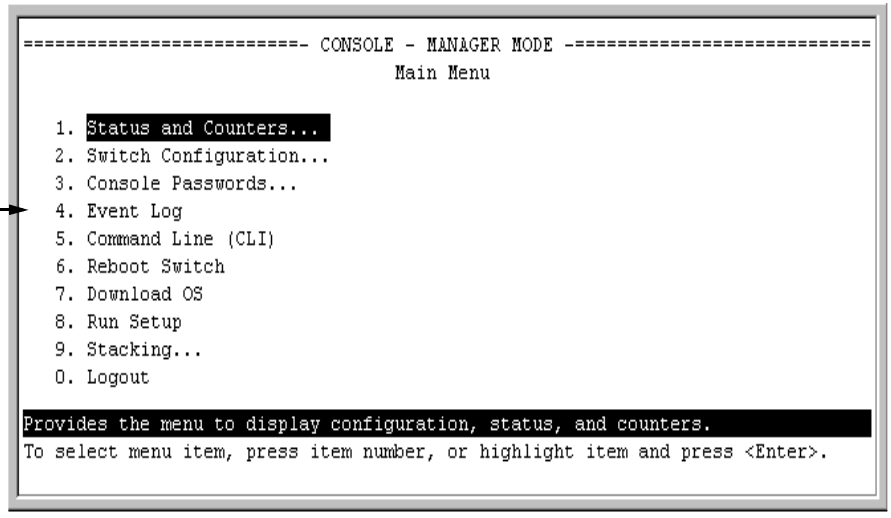



**Figure 2-1. The Reboot Switch Option in the Main Menu**

**Rebooting To Activate Configuration Changes.** Configuration changes for most parameters become effective as soon as you save them. However, you must reboot the switch in order to implement a change in the **Maximum VLANs to support** parameter.

(To access these parameters, go to the Main menu and select **2. Switch Configuration**, then **8. VLAN Menu**, then **1. VLAN Support**.)

If configuration changes requiring a reboot have been made, the switch displays an asterisk (*) next to the menu item in which the change has been made. For example, if you change and save parameter values for the **Maximum VLANs to support** parameter, an asterisk appears next to the **VLAN Support** entry in the VLAN Menu screen, and also next to the the **Switch Configuration . . .** entry in the Main menu, as shown in figure 4-6:

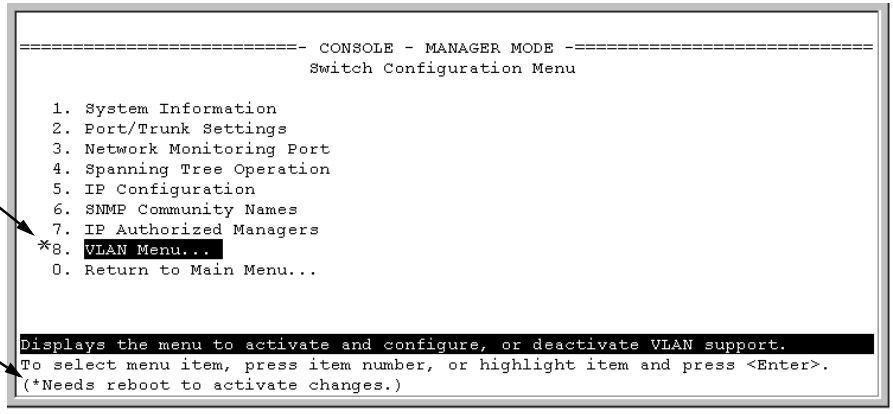



**Figure 2-2. Indication of a Configuration Change Requiring a Reboot**

## Using the Web Browser Interface To Implement Configuration Changes

You can use the web browser interface to simultaneously save and implement a subset of switch configuration changes without having to reboot the switch. That is, when you save a configuration change (in most cases, by clicking on [Apply Changes] or [Apply Settings], you simultaneously change both the running-config file and the startup-config file.

**Note**

If you reconfigure a parameter in the CLI and then go to the browser interface without executing a **write memory** command, those changes will be saved to the startup-config file if you click on [Apply Changes] or [Apply Settings] in the web browser interface.

# Daylight Savings Time

The SMC6624M switch provides a way to automatically adjust the system clock for Daylight Savings Time (DST) changes. In addition to the value "none" (no time changes), there are five pre-defined settings, named:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The pre-defined settings follow these rules:

**Alaska:**

- Begin DST at 2am the first Sunday on or after April 24th.
- End DST at 2am the first Sunday on or after October 25th.

**Canada and Continental US:**

- Begin DST at 2am the first Sunday on or after April 1st.
- End DST at 2am the first Sunday on or after October 25th.

**Middle Europe and Portugal:**

- Begin DST at 2am the first Sunday on or after March 25th.
- End DST at 2am the first Sunday on or after September 24th.

**Southern Hemisphere:**

- Begin DST at 2am the first Sunday on or after October 25th.
- End DST at 2am the first Sunday on or after March 1st.

**Western Europe:**

- Begin DST at 2am the first Sunday on or after March 23rd.
- End DST at 2am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows the user to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change. The menu interface screen looks like this (all month/date entries are at their default values):

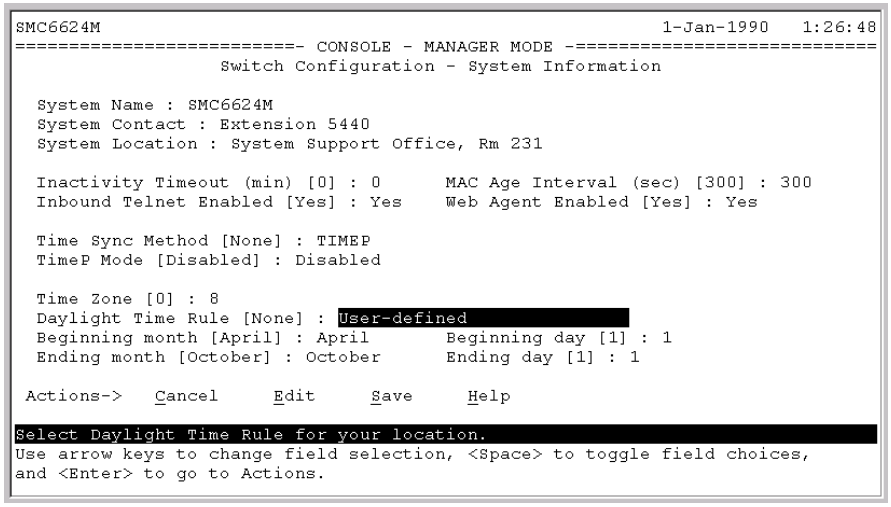



**Figure D-1. Menu Interface with "User-Defined" Daylight Time Rule Option**

Before configuring a "User defined" Daylight Time Rule, it is important to understand how the switch treats the entries. The switch knows which dates are Sundays, and uses an algorithm to determine on which date to change the system clock, given the configured "Beginning day" and "Ending day":

- If the configured day is a Sunday, the time changes at 2am on that day.
- If the configured day is not a Sunday, the time changes at 2am on the first Sunday after the configured day.

This is true for both the "Beginning day" and the "Ending day".

With that algorithm, one should use the value "1" to represent "first Sunday of the month", and a value equal to "number of days in the month minus 6" to represent "ast Sunday of the month". This allows a single configuration for every year, no matter what date is the appropriate Sunday to change the clock.

## Numerics

802.1Q VLAN standard … 9-99
802.3u auto negotiation standard … 6-2

## A

access
    manager … 8-5
    operator … 8-5
access levels, authorized IP managers … 7-29
Actions line … 2-8–2-10
    location on screen … 2-8
active path … 9-99
address
    authorized for port security … 7-8
address table, port … 10-11
address, network manager … 8-3
advertisement … 9-74
alert log … 4-15
    alert types … 4-16
    sorting the entries … 4-15
analysis, traffic … 8-1
APNIC … 5-14
Asia-Pacific NIC … 5-14
asterisk … 2-9
authentication trap … 8-9, 8-11
authentication trap, configuring … 8-11
authorized addresses
    for IP management security … 7-29
    for port security … 7-8
authorized IP managers
    access levels … 7-29
    building IP masks … 7-34
    configuring in browser interface … 7-33–7-34
    configuring in console … 7-31
    definitions of single and multiple … 7-29
    effect of duplicate IP addresses … 7-37
    IP mask for multiple stations … 7-35
    IP mask for single station … 7-34
    IP mask operation … 7-30
    operating notes … 7-37
    overview … 7-28
    troubleshooting … 7-37
auto
    See GVRP
auto negotiation … 6-3
auto port setting … 9-89
Auto-10 … 6-10, 6-13
auto-discovery … 8-4
auto-negotiation … 6-2

## B

bandwidth
    displaying utilization … 4-12
bandwidth savings, with IGMP … 9-95
blocked link from STP operation … 9-107
blocked port
    from IGMP operation … 9-89
    from STP operation … 9-105
Bootp … 5-2, 5-10, 8-1
    Bootp table file … 5-12
    Bootptab file … 5-12
    effect of no reply … 11-5
    operation … 5-12
    using with Unix systems … 5-12
Bootp/DHCP differences … 5-11
BPDU … 9-74
bridge protocol data unit … 9-74
broadcast domain … 9-48
broadcast limit … 6-3
broadcast storm … 6-10, 9-99, 11-7
browsers … 4-3

## C

Clear button … 4-9
    restoring factory default configuration … 11-19
    to delete password protection … 7-5
CLI
    context level … 6-7
command line interface
    *See* CLI
communities, SNMP … 8-6
configuration … 2-6, 9-105
    Bootp … 5-12
    console … 5-15
    copying … A-9
    download … A-1
    factory default … 5-1, 9-55, 9-60, 9-100, C-6
    IP … 5-2
    network monitoring … 10-20
    permanent … C-4
    permanent change defined … C-2
    port … 6-1
    port security … 7-9
    port trunk groups … 6-1

quick … 2-7
restoring factory defaults … 11-19
saving from menu interface … 2-9
serial link … 5-15
SNMP … 8-3, 8-5
spanning tree … 9-99
spanning tree protocol … 9-105
startup … 2-9
system … 5-20
Telnet access configuration … 5-15
transferring … A-9
trap receivers … 8-9
viewing … C-3
VLAN … 9-48
web browser access … 5-15
configuration file
browsing for troubleshooting … 11-17
connection inactivity time … 7-3
console … 11-5
configuring … 5-15
ending a session … 2-4
features … 1-2
Main menu … 2-6
navigation … 2-8–2-9
operation … 2-9
starting a session … 2-3
status and counters access … 2-6
troubleshooting access problems … 11-3
console, for configuring
authorized IP managers … 7-31
CPU utilization … 10-4

## D

date format … 11-10
date,configure … 5-24
default gateway … 5-2
default trunk type … 6-16
Device Passwords Window … 4-7
DHCP … 5-10
address problems … 11-5
effect of no reply … 11-5
DHCP/Bootp differences … 5-11
DHCP/Bootp process … 5-11
diagnostics tools … 11-13
browsing the configuration file … 11-17
ping and link tests … 11-13
DNS name … 4-4
domain … 9-55, 9-60
Domain Name Server … 4-4
download
switch-to-switch … A-4
troubleshooting … A-8
Xmodem … A-6
download OS … A-4
download, TFTP … A-1–A-3
duplicate IP address
effect on authorized IP managers … 7-37
duplicate MAC address … 9-73, 11-9
Dyn1
See LACP

## E

ending a console session … 2-4
event log … 2-6, 11-10
intrusion alerts … 7-25
navigation … 11-11
severity level … 11-10
use during troubleshooting … 11-10

## F

factory default configuration
restoring … 11-19, C-6
failure, OS download … A-8
Fast EtherChannel
*See* FEC
fast mode
spanning tree … 9-106
fault-tolerance … 6-11
FEC
benefits … 6-26
filters
effect of IGMP … 9-98
maximum allowed … 9-98
firmware version … 10-4
flash memory … 2-9
flow control … 6-3
flow control, terminal … 5-15
forbid
See GVRP
format, date … 11-10
format, time … 11-10
forwarding port, IGMP … 9-89

## G


GARP
    See GVRP
gateway … 5-2, 5-4
gateway (IP) address … 5-3, 5-5
GVRP
    advertisement … 9-75, 9-87
    advertisement, defined … 9-74
    advertisement, responses to … 9-76
    advertisements, generating … 9-80
    auto … 9-79
    benefit … 9-74
    block … 9-78
    BPDU … 9-75
    CLI, configuring … 9-83
    common VID required … 9-75
    configurable port options … 9-77
    configuring learn, block, disable … 9-78
    convert dynamic to static … 9-77
    converting to static VLAN … 9-74
    disable … 9-78
    dynamic VLAN and reboots … 9-86
    dynamic VLANs always tagged … 9-75
    forbid … 9-79
    GARP … 9-74
    general operation … 9-75
    IP addressing … 9-77
    learn … 9-78
    learn, block, disable … 9-79
    menu, configuring … 9-81
    non-GVRP aware … 9-86
    non-GVRP device … 9-86
    operating notes … 9-86
    per-port static configuration … 9-75
    port control options … 9-80
    port-leave from dynamic … 9-80
    reboot, switch … 9-80
    recommended tagging … 9-80
    required VLAN … 9-75
    standard … 9-74
    tagged, dynamic VLAN … 9-75
    unknown VLAN … 9-80
    unknown VLAN, options … 9-77
    VLAN behavior … 9-52
    VLAN, dynamic adds … 9-58


## H


Help … 2-10
Help line, about … 2-8
Help line, location on screens … 2-8
host-only … 9-73


## I


ICANN … 5-14
IEEE 802.1d … 9-99, 11-7
IEEE 802.3ab … 6-3
IGMP
    benefits … 9-88
    configuration … 9-94
    configure per VLAN … 9-89
    effect on filters … 9-98
    example … 9-95–9-97
    high-priority forwarding … 9-89
    host not receiving … 11-6
    IP address required … 9-89
    IP multicast address range … 9-98
    leave group … 9-95
    maximum address count … 9-98
    multicast group … 9-95, 9-97
    multimedia … 9-88
    not working … 11-6
    operation … 9-94–9-95
    port states … 9-89
    query … 9-95
    report … 9-95
    statistics … 10-16
    status … 9-95
    traffic … 9-89
inactivity timeout … 5-16
Inbound Telnet Enabled parameter … 11-4
inconsistent value, message … 7-17
interfaces listed … 1-1
intrusion alarms
    entries dropped from log … 7-27
    event log … 7-25
    prior to … 7-27
Intrusion Log
    prior to … 7-23, 7-25
invalid input … 3-12
IP
    address for IGMP … 9-89
    authorized IP managers … 7-28
    CLI access … 5-6

configuration … 5-2
DHCP/Bootp … 5-2
duplicate address … 11-5
duplicate address, DHCP network … 11-5
effect when address not used … 5-9
gateway … 5-2
gateway (IP) address … 5-3
global assignment … 5-14
globally assigned addressing … 5-14
menu access … 5-4
stacking … 5-4
subnet mask … 5-2, 5-6
using for web browser interface … 4-4
web access … 5-9
IP host-only … 9-73
IP masks
building … 7-34
for multiple authorized manager stations … 7-35
for single authorized manager station … 7-34
operation … 7-30
IP, for SNMP … 8-1
IPX
network number … 10-5


## J


Java … 4-4


## L


LACP
active … 6-21, 6-24
CLI access … 6-17
default port operation … 6-24
described … 6-12, 6-23
Dyn1 … 6-13
dynamic … 6-23
enabling dynamic trunk … 6-21
full-duplex required … 6-3, 6-10, 6-23
IGMP … 6-25
no half-duplex … 6-26
outbound traffic distribution … 6-27
overview … 6-11
passive … 6-21, 6-24
removing port from dynamic trunk … 6-22
restrictions … 6-25
standby link … 6-23
status, terms … 6-24
STP … 6-25
VLANs … 6-25
learning bridge … 5-1
leave group
*See* IGMP
legacy VLAN … 9-50
link speed, port trunk … 6-10
link test … 11-13
for troubleshooting … 11-13
link, serial … 5-15
load balancing
*See* port trunk
loop, network … 6-10, 9-99, 9-105
lost password … 4-9


## M


MAC address … 5-12, 10-4, B-1
duplicate … 9-73, 11-7, 11-9
learned … 10-10–10-11
port … B-1–B-2
switch … B-1
VLAN … 9-72, B-1
management
interfaces described … 1-1
manager access … 8-5
manager password … 4-7–4-8, 7-2, 7-4
Manual, IP address … 5-6
media type, port trunk … 6-10
memory
flash … 2-9
startup configuration … 2-9
menu interface
configuration changes, saving … 2-9
message
inconsistent value … 7-17
VLAN already exists … 9-66
MIB … 8-3
MIB listing … 8-2
MIB, SMC proprietary … 8-2
MIB, standard … 8-2
Microsoft Internet Explorer … 4-4
mirroring
See port monitoring.
Monitor parameter … 10-22
monitoring a VLAN … 10-23
monitoring traffic … 10-20
monitoring, traffic … 8-1

multicast group
*See* IGMP
multimedia
*See* IGMP
multiple VLAN … 8-1
multi-port bridge … 5-1

## N

navigation, console interface … 2-8–2-9
navigation, event log … 11-12
Netscape … 4-4
network management functions … 8-4
network manager address … 8-3
network monitoring
traffic overload … 10-20
VLAN monitoring parameter … 10-23
Network Monitoring Port screen … 10-20
network slow … 11-5
notes on using VLANs … 9-54

## O

operating notes
authorized IP managers … 7-37
port security … 7-26
operator access … 8-5
operator password … 4-7–4-8, 7-2, 7-4
OS
version … A-4–A-6
OS download
failure indication … A-8
switch-to-switch download … A-4
troubleshooting … A-8
using TFTP … A-2
out-of-band … 1-2

## P

password … 4-7–4-8
browser/console access … 7-3
case-sensitive … 7-4
creating … 4-7
delete … 2-6, 4-9, 7-4
deleting with the Clear button … 7-5
if you lose the password … 4-9, 7-5
incorrect … 7-3
length … 7-4
lost … 4-9
manager … 4-7
operator … 4-7
set … 2-6
setting … 4-8, 7-3
using to access browser and console … 4-8
path cost … 9-106
ping test … 11-13
for troubleshooting … 11-13
port
1000 Mbps, full-duplex only … 6-3
address table … 10-11
Address Table screen … 9-73
auto negotiation … 6-3
auto, IGMP … 9-89
auto-negotiation … 6-2
blocked by STP operation … 9-105
blocked, IGMP … 9-89
CLI access … 6-5
context level … 6-7
cost
*See* spanning tree protocol.
counters … 10-7
counters, reset … 10-7
fiber-optic … 6-3
forwarding, IGMP … 9-89
full-duplex, LACP … 6-3
MAC address … B-2–B-3
menu access … 6-4
monitoring … 9-72
numbering … 6-1
security configuration … 7-7
See port trunk
speed change, transceiver … 6-3
state, IGMP control … 9-89
traffic patterns … 10-7
utilization … 4-12
web browser interface … 4-12
web browser access … 6-8
Port Configuration … 6-1
port security
authorized address definition … 7-8
basic operation … 7-7
configuring … 7-9
configuring in browser interface … 7-20, 7-26
event log … 7-25
intrusion alert … 6-2
notice of security violations … 7-20

operating notes … 7-26
overview … 7-7
port trunk restriction … 6-10
prior to … 7-27
proxy web server … 7-27
trunk restriction … 6-14
port trunk … 6-9
bandwidth capacity … 6-9
caution … 6-10, 6-15, 6-22
CLI access … 6-17
default trunk type … 6-16
enabling dynamic LACP … 6-21
FEC … 6-12, 6-26
IGMP … 6-14
LACP … 6-3
LACP, full duplex required … 6-10
limit … 6-9
link requirements … 6-10
media requirements … 6-13
media type … 6-10
menu access to static trunk … 6-15
monitor port restrictions … 6-14
nonconsecutive ports … 6-9
port security restriction … 6-14
removing port from static trunk … 6-20
requirements … 6-13
SA/DA … 6-27
See also LACP
See LACP
spanning tree protocol … 6-14
static trunk … 6-13
static trunk, overview … 6-11
STP … 6-14
STP operation … 6-13
traffic distribution … 6-13
Trk1 … 6-13
trunk (non-protocol) option … 6-12
trunk option described … 6-26
types … 6-12
VLAN … 6-14, 9-72
VLAN operation … 6-13
web browser access … 6-22
port trunk group
interface access … 6-1
power interruption, effect on event log … 11-10
primary VLAN
*See* VLAN
prior to … 7-23, 7-25, 7-27
priority … 9-89
*See* spanning tree
proprietary MIB … 8-2
proxy
web server … 7-27
public SNMP community … 8-3–8-4

## Q

query
*See* IGMP
quick configuration … 2-7
quick start … 5-3

## R

reboot … 2-7, 2-9, 2-11, 9-80
reboot, actions causing … C-2
reconfigure … 2-9
redundant path … 9-99, 9-105
spanning tree … 9-100
report
*See* IGMP
reset … 2-11, C-8
Reset button
restoring factory default configuration … 11-19
reset port counters … 10-7
resetting the switch
factory default reset … 11-19
restricted access … 8-5
restricted write access … 8-5
RFC
*See* MIB
RFC 1213 … 8-2
RFC 1493 … 8-2
RFC 1515 … 8-2
RFC 1573 … 8-2
RFC 1757 … 8-2
RIPE NCC … 5-14
RMON … 8-2
RMON groups supported … 8-12
router … 9-94
gateway … 5-5
RS-232 … 1-2

## S

security … 4-9, 5-15

authorized IP managers … 7-28
per port … 7-7
security violations
notices of … 7-20
Self Test LED
behavior during factory default reset … 11-19
serial number … 10-4
server
access failure … 9-100
Timep … 5-5
setting a password … 7-3
setup screen … 5-3
severity code, event log … 11-10
slow network … 11-5
SNMP … 8-1
CLI commands … 8-5
communities … 8-3, 8-5–8-6
Communities screen … 8-5
community
configure … 8-3
IP … 8-1
public community … 8-4–8-5
restricted access … 8-5
traps … 8-2
software version … 10-4
sorting alert log entries … 4-15
spanning tree … 9-99
blocked link … 9-107
blocked port … 9-105
causing duplicate MAC address … 9-73
description of operation … 9-105
enabling from the browser interface … 9-105
fast mode … 9-106
global information … 10-14
information screen … 10-14
link priority … 9-100
port cost … 9-105
port priority automatic setting … 9-105
problems related to … 11-7
statistics … 10-14
using with port trunking … 6-14
VLAN effect on … 9-71
stacking
benefits … 9-2–9-3
primary … 9-46
standard MIB … 8-2
starting a console session … 2-3
static VLAN, convert to … 9-74
statistical sampling … 8-1
statistics … 2-6, 10-2
statistics, clear counters … 2-11, C-8
status and counters
access from console … 2-6
status and counters menu … 10-3
status overview screen … 4-5
STP
See spanning tree.spanning tree
server access failure … 9-100
subnet … 9-95
subnet address … 9-48
subnet mask … 5-4, 5-6
*See also* IP
Sun workstation … 9-73
support
URL Window … 4-10
switch console
*See* console
switch setup menu … 2-7
switch-to-switch download … A-4
system configuration screen … 5-20
System Name parameter … 5-21


## T


tagged VLAN
*See* VLAN
TCP/IP reference book … 5-14
Telnet … 2-3
Telnet, enable/disable … 5-16
Telnet, problem … 11-4
terminal access, lose connectivity … 5-18
terminal type … 5-15
TFTP
download … A-1, A-3
OS download … A-2
threshold setting … 8-4
time format … 11-10
Time Protocol parameter … 5-5
time server … 5-2
time, configure … 5-24
TimeP … 5-2–5-4
Timep … 5-3, 5-5
Timep Poll Interval … 5-5
Timep Server … 5-5
Time-To-Live … 5-2, 5-4
top talker … 6-28

traffic analysis … 8-1
traffic monitoring … 8-1, 8-4
traffic, monitoring … 10-20
traffic, port … 10-7
transceiver, fiber-optic … 6-3
transceiver, speed change … 6-3
trap
  authentication … 8-9
  authentication trap … 8-11
  CLI access … 8-10
  event levels … 8-9
  limit … 8-9
  receiver … 8-9
  SNMP … 8-9
  Trap Receivers Configuration screen … 8-9
trap receiver … 8-3, 8-9
  configuring … 8-11
troubleshooting
  approaches … 11-2
  authorized IP managers … 7-37
  browsing the configuration file … 11-17
  console access problems … 11-3
  diagnosing unusual network activity … 11-5
  diagnostics tools … 11-13
  OS download … A-8
  ping and link tests … 11-13
  restoring factory default configuration … 11-19
  unusual network activity … 11-5
  using the event log … 11-10
  web browser access problems … 11-3
trunk
  *See* port trunk
trunk group
  FEC … 6-24
TTL … 5-2, 5-4
types of alert log entries … 4-16

## U

unauthorized access … 8-11
Universal Resource Locator
  *See* URL
Unix, Bootp … 5-12
unrestricted write access … 8-5
unusual network activity … 11-5
up time … 10-4
URL
  support … 4-10
user name
  cleared … 7-5
user name, using for browser or console access … 4-7, 4-9
using the passwords … 4-8
utilization, port … 4-12

## V

value, inconsistent … 7-17
version, OS … A-4–A-6
VID
  See <default para text>VLAN
virtual stacking
  transmission interval range … 9-15–9-16
VLAN … 5-3, 9-48, 9-71–9-73, 10-22–10-23, 11-9, B-1
  802.1Q … 9-107
  address … 8-1
  Bootp … 5-12
  configuring Bootp … 5-12
  convert dynamic to static … 9-74
  DEFAULT_ VLAN … 9-51
  deleting … 9-73
  device not seen … 11-8
  DHCP, primary VLAN … 9-52
  duplicate MAC address … 9-73
  dynamic … 9-48, 9-54–9-55, 9-60
  effect on spanning tree … 9-71
  event log entries … 11-10
  ID … 3-14
  IGMP configuration … 9-89
  limit … 9-55, 9-60
  link blocked … 11-7
  MAC address … 9-72
  monitoring … 10-1, 10-23
  multiple … 8-1
  multiple VLANs on port … 9-69
  network monitoring … 10-20
  notes on using … 9-54
  number allowed, including dynamic … 9-58
  OS download … A-2
  port assignment … 9-58
  port configuration … 9-70, 11-8
  port monitoring … 9-72
  port restriction … 9-73
  port trunk … 9-72
  primary … 5-2, 9-8, 9-33, 9-46, 9-52
  primary VLAN … 9-51

primary, CLI command … 9-61, 9-63
primary, select in menu … 9-56
primary, web configure … 9-66
primary, with DHCP … 9-54
reboot required … 2-7
restrictions … 9-73
See GVRP
spanning tree operation … 9-107
stacking, primary VLAN … 9-52
static … 9-48, 9-52, 9-55, 9-60
support enable/disable … 2-7
switch capacity … 9-48
tagged … 9-49
tagging … 9-67, 9-69
tagging broadcast, multicast, and unicast traffic … 11-8
unknown VLAN … 9-80
untagged … 9-50, 9-59
VID … 9-48, 9-69
VID, default VLAN … 9-52
VLAN already exists, message … 9-66
VLAN ID
See VLAN … 3-14
VT-100 terminal … 5-15

## W

warranty … 1-i
web agent enabled … 4-1
web agent,
advantages … 1-4
web browser access configuration … 5-15
web browser enable/disable … 5-16
web browser interface
access parameters … 4-7
alert log … 4-5, 4-15
alert log details … 4-17
alert types … 4-16
bandwidth adjustment … 4-13
bar graph adjustment … 4-13
disable access … 4-1
enabling … 4-4
error packets … 4-12
features … 1-4
first-time install … 4-6
first-time tasks … 4-6
main screen … 4-11
overview … 4-11
Overview window … 4-11
password lost … 4-9
password, setting … 4-8
port status … 4-14
port utilization … 4-12
port utilization and status displays … 4-12
screen elements … 4-11
security … 4-1, 4-7
standalone … 4-4
status bar … 4-17
status indicators … 4-18
status overview screen … 4-5
system requirements … 4-3–4-4
troubleshooting access problems … 11-3
web browser interface, for configuring
port security … 7-26
authorized IP managers … 7-33–7-34
IGMP … 9-94
port security … 7-20
STP … 9-105
web server, proxy … 7-27
write access … 8-5
write memory … 9-86

## X

Xmodem OS download … A-6
XNS … 9-73

**FOR TECHNICAL SUPPORT, CALL:**

From U.S.A. and Canada (24 hours, 7 days a week)
(800) SMC-4-YOU; (949) 707-2400; (949) 707-2460 (Fax)
From Europe (8:00 AM - 5:30 PM UK Greenwich Mean Time)
44 (0) 1188 748740; 44 (0) 1189 748741 (Fax)

**INTERNET**

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
Driver updates:
http://www.smc.com/support.html
World Wide Web:
http://www.smc.com/
FTP Site:
ftp.smc.com

**FOR LITERATURE OR ADVERTISING RESPONSE, CALL:**

| | | |
|---|---|---|
| U.S.A. and Canada: | (800) SMC-4-YOU; | Fax (949) 707-2460 |
| Spain: | 34-93-477-4920; | Fax 34-93-477-3774 |
| UK: | 44 (0) 1188 748700; | Fax 44 (0) 1189 748701 |
| Southern Europe: | 33 (1) 41.18.68.68; | Fax 33 (1) 41.18.68.69 |
| Central/Eastern Europe: | 49 (0) 89 92861-200; | Fax 49 (0) 89 92861-230 |
| Nordic: | 46 (8) 564 33145; | Fax 46 (8) 87 62 62 |
| Middle East: | 971-48818410; | Fax 971-48817993 |
| South Africa: | 27 (0) 11-3936491; | Fax 27 (0) 11-3936491 |
| PRC: | 86-10-6235-4958; | Fax 86-10-6235-4962 |
| Taiwan: | 886-2-2659-9669; | Fax 886-2-2659-9666 |
| Asia Pacific: | (65) 238 6556; | Fax (65) 238 6466 |
| Korea: | 82-2-553-0860; | Fax 82-2-553-7202 |
| Japan: | 81-45-224-2332; | Fax 81-45-224-2331 |
| Australia: | 61-2-9416-0437; | Fax 61-2-9416-0474 |
| India: | 91-22-8204437; | Fax 91-22-8204443 |

SMC®
Networks

6 Hughes
Irvine, CA 92618
Phone: (949) 707-2400

Model Numbers: SMC6624M
Publication Number: 150000001100A
Revision Number: F2.05 E072001-R01